全国计算机技术与软件专业技术资格（水平）考试参考用书

网络管理员考试同步辅导
(下午科目)(第2版)

全国计算机专业技术资格考试办公室推荐
蒋道霞　李佐勇　胡丽娜　主编

清华大学出版社
北京

全国计算机技术与软件专业技术资格(水平)考试参考用书

网络管理员考试同步辅导

(下午科目)(第 2 版)

蒋道霞　李佐勇　胡丽娜　主编

清华大学出版社
北　京

内 容 简 介

本书是按照人事部(现为人力资源和社会保障部)、信息产业部(现为工业和信息化部)最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材编写的考试辅导书。全书共分为 5 章，内容包括：小型局域网的构建与综合布线、局域网服务器的安装和配置、网络安全设置、网络管理与故障处理、Web 网站建设，主要从考试大纲要求、考点辅导、典型例题分析、本章小结和达标训练几个方面对各部分内容加以系统阐释。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合备考网络管理员的考生使用，也可作为高等院校或培训班的教材。

图书在版编目(CIP)数据

网络管理员考试同步辅导(下午科目)/蒋道霞，李佐勇，胡丽娜主编. —2 版. —北京：清华大学出版社，2010.6
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 978-7-302-22512-6

Ⅰ. 网…　Ⅱ. ①蒋…　②李…　③胡…　Ⅲ. 计算机网络—系统管理—工程技术人员—资格考核—自学参考资料　Ⅳ. TP393

中国版本图书馆 CIP 数据核字(2010)第 066343 号

责任编辑：章忆文　张丽娜
装帧设计：何凤霞
责任校对：李玉萍
责任印制：

出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　**印　张：**25.5　**字　数：**611 千字
版　次：2010 年 6 月第 2 版　**印　次：**2010 年 6 月第 1 次印刷
印　数：1~4000
定　价：39.00 元

产品编号：

再 版 前 言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了 20 多年，在社会上产生了很大的影响，其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求，人事部(现为人资源和社会保障部)、信息产业部(现为工业和信息化部)在 2004 年决定将考试的级别拓展到计算机技术与软件各个方面，将网络程序员级别考试改为网络管理员级别考试，2009 年又对网络管理员级别考试大纲进行了重新调整，以满足社会对各种信息技术人才的需要。本书第 1 版自 2005 年出版以来，被众多考生选用为考试参考教材，多次重印，深受广大读者好评。为了帮助考生复习迎考，根据 2009 年考试大纲的最新变化及网络新技术的发展，本书对第 1 版进行了修订。主要修订内容如下。

(1) 知识点更新。2009 年新大纲对知识点有所调整与变动，使其更注重实践性。本书在第 1 版的基础上，严格按照 2009 年新版大纲，对知识点做了彻底的更新，更符合新大纲新教程对考试的要求。

(2) 结构调整。参考最新指定官方教程、最新考试大纲及最新题型编写章节、节名，便于考生使用《网络管理员教程(第 3 版)》同步复习，同时更加突出重点与难点，针对性强，可减轻考生复习的工作量。

(3) 例题与习题更新。对书中原有例题与习题进行了彻底更新，最近 4 年(2006—2009 年)8 次考试真题全部分类解析到例题中，并在其中增加了根据最新考试大纲精心设计的例题，这些例题均具有典型性和代表性，而将 2005 年两次考试真题全部分类归入同步练习中。这样考生能从以前的考题中，更好地了解考试的难度与广度。

(4) 更加突出重点。第 2 版沿袭前一版的框架，每一小节分为 4 个模块：考点辅导、典型例题分析、同步练习、同步练习参考答案。其中，考点辅导部分主要以专题的方式，重点介绍网络管理员上午考试所需的各个方面的知识；典型例题分析是本书的重点，它详尽细致地剖析了所有近 4 年(2006—2009 年)的真题和例题；同步练习中的每一道题都配有标准答案；此外，每章还配有一定数量的习题及答案，对读者所学的知识和能力可起到巩固、拓展和提高的作用。

(5) 概念更清晰，能覆盖所有大纲考点，并突出重难点。

(6) 精选书中所有例题与习题，确保所有题目符合考纲要求。例题选取典型、有梯度、有广度，分析更详尽；题目的难易度、分布率与真实考试相当；题目答案正确、解析科学；无重复题目、雷同题目。

本书非常适合备考网络管理员的考生使用，也可作为高等学校相关专业或培训班的教材。

本书第 1 版由李文龙、施宁、陶安、俞永达、张伍荣等编写。第 2 版是对第 1 版的修订与升级，具体由蒋道霞、李佐勇、胡丽娜完成编写与升级工作。此外，参与本书编写的还有陈海燕、陈智、程勇、郭龙源、何光明、徐军、马常霞、祁云嵩、申继年、孙建东、

王珊珊、许勇、张宏等。在此对原作品的全体参与人员表示衷心的感谢。

在本书的编写过程中，参考了许多相关的书籍和资料，目录详见参考文献，本书从中汲取了许多营养，在此表示感谢。需要特别提出感谢的是来自互联网的各位不知姓名的网友们的无私奉献，正是由于你们，才使本书的内容更完善、更详尽。

由于作者水平所限，书中难免存在错漏和不妥之处，敬请广大读者批评指正。

编　者

网络管理员考试(下午)考点分布导航图

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2006.05	2006.11	2007.05	2007.11	2008.05	2008.11	2009.05	2009.11			
第 1 章 小型局域网的构建与综合布线	1.1 局域网组网的设计	相关考题结合“1.2 局域网组网技术及设备选择”一起考。								**1. 未变动的大纲要求：** ①组网技术选择； ②组网设备选择及部署； ③设备配置和管理； ④划分 VLAN； ⑤综合布线； ⑥IP 地址、子网掩码的规划配置。 **2. 新增的大纲要求：** ★网络规划； ★命令行接口访问交换机和路由器； ★Web 方式访问交换机和路由器； ★VLAN 配置； ★路由器路由协议配置； ★广域联网。 **3. 删除的大纲要求：** ①综合布线概念、组成、设计及依据的标准； ②综合布线基础环境准备； ③线缆及相关硬件的选择与安装； ④综合布线系统的性能指标及测试流程。 **4. 对大纲变化的说明：** 考试大纲新增了“交换机与路由器的基本配置”内容，同时弱化了“综合布线”内容，而“综合布线”相关考题又未曾出现过。考生应注意复习重点的变化。	**1. 考题分布：** 通常出现在网络管理员考试(下午科目)的第 1 题或者第 2 题。 **2. 阅读提示：** 本章的“1.1 局域网组网的设计”，“1.2 局域网组网技术及设备选择”，“1.3 以太网交换机的部署”和“1.4 交换机与路由器的基本配置”对应《网络管理员教程(第 3 版)》(以下简称“教程”)的“3.2 以太网”、“3.3 交换机与路由器的基本配置”和“3.4 综合布线”，“1.5 IP 地址及其规划”对应教程的“1.4.3 IP 地址”。考生可以对照教程相关内容进行同步复习。 **3. 补充说明：** 但需要注意的是，增加了大纲未明确指出，教程未提及，但考试中遇到的重要考点。 ※组网设备选择及部署。请考生留意此部分内容。	本章节考点分值约占总考分的 12%。考查在指定网络环境要求下进行网络设计，包括设计拓扑结构、所用的设备类型、线缆类型、网络排错等。有时也考查对原网络的升级。高频考点为： ◆局域网组网技术及设备选型； ◆交换机和路由器的基本配置； ◆IP 地址以及子网掩码的规划。
	1.2 局域网组网技术及设备选择		路由器和交换机(3 分)		路由器和交换机(4 分)，双绞线(3 分)		交换机(2 分)					
	1.3 以太网交换机的部署		交换机的控制台端口(2 分)									
	1.4 交换机与路由器的基本配置	2009 年考试大纲新增加的内容，至今还没有出过考题。										
	1.5 综合布线	2009 年考试大纲弱化的知识点，至今还没有出过考题。										
	1.6 IP 地址及其规划	IP 地址以及子网掩码(6 分)		配置 Internet 协议属性参数(15 分)	IP 地址以及子网掩码(4 分)，NAT 的功能(4 分)		IP 地址以及子网掩码(13 分)	IP 地址以及子网掩码(11 分)	IP 地址以及子网掩码(8 分)，路由表(5 分)			

续表

<table>
<tr><th rowspan="2">章</th><th rowspan="2">节</th><th colspan="8">历年真题分布</th><th rowspan="2">大纲要求</th><th rowspan="2">阅读链接</th><th rowspan="2">命题预测</th></tr>
<tr><th>2006.05</th><th>2006.11</th><th>2007.05</th><th>2007.11</th><th>2008.05</th><th>2008.11</th><th>2009.05</th><th>2009.11</th></tr>
<tr><td rowspan="7">第 2 章 局域网服务器的安装和配置</td><td>2.1 操作系统的安装</td><td>Windows Server 2003 的安装(15 分)</td><td></td><td></td><td></td><td>Linux 操作系统的安装以及 NAT 的功能(15 分)</td><td>IE 浏览器的基本知识(15 分)</td><td></td><td></td><td rowspan="7">1. 未变动的大纲要求：
①Windows DNS 服务器的配置和维护；
②Windows 电子邮件服务器的配置和维护；
③Windows FTP 服务器的配置和维护；
④Windows 代理服务器的配置和维护；
⑤Windows DHCP 服务器的配置和维护。
2. 新增的大纲要求：
Windows WEB 服务器的配置和维护。
3. 删除的大纲要求：
Linux 系统下 DNS 服务器、电子邮件服务器、FTP 服务器、代理服务器和 DHCP 服务器的规划、设置和维护。
4. 对大纲变化的说明：
考试大纲新增“Windows Web 服务器的配置和维护”考点，该考点在往年考题中已经出现，现在在考试大纲中明确是合理的大纲调整。同时，Linux 系统下的服务器配置在考试大纲中已经删除。考生应该注意复习重点的转移。</td><td rowspan="7">1. 考题分布：
通常出现在网络管理员考试(下午科目)的第 2 题或者第 3 题，也偶尔出现在第 1 题。
2. 阅读提示：
本章的“2.1 操作系统的安装”对应教程“4.2 Windows Server 2003 的安装与配置”和“4.3 Red Flag Server 4.0”；“2.2 DNS 服务器配置”对应教程“5.2 DNS 服务器的配置”；“2.3 电子邮件服务”对应教程“5.5 电子邮件服务器的配置”；“2.4 FTP 服务器”和“2.5 Web 服务器配置”对应教程“5.1 IIS 服务器配置”；“2.6 代理服务器配置”对应教程“5.6 代理服务器”；“2.7 DHCP 服务器的配置”对应教程“5.3 DHCP 服务器的配置”。考生可以对照教程的相关内容进行同步复习。</td><td rowspan="7">本章节考点分值约占总考分的 43%。考生应充分重视本章的复习。通常考查各种服务器的配置实现。高频考点为：
◆ 常见操作系统的安装；
◆ Windows FTP 服务器的配置；
◆ Windows DNS 服务器的配置；
◆ Windows DHCP 服务器的配置。</td></tr>
<tr><td>2.2 DNS 服务器配置</td><td></td><td></td><td></td><td>Windows Server 2003 系统 DNS 服务器的配置过程(13 分)，测试 DNS 配置成功情况(2 分)</td><td></td><td></td><td>域名服务器的类型(3 分)，域名服务器的功能(3 分)，DNS 服务的启动和停止(4 分)，域名服务器的配置(3 分)，DNS 故障排除(2 分)</td><td></td></tr>
<tr><td>2.3 电子邮件服务</td><td></td><td></td><td></td><td></td><td></td><td></td><td>电子邮件服务器的配置过程(15 分)</td><td></td></tr>
<tr><td>2.4 FTP 服务器</td><td>FTP 服务器的端口(3 分)，配置 FTP 服务器的过程(6 分)，连接 FTP 服务器的命令(6 分)</td><td></td><td></td><td>FTP 协议和 TCP 协议(4 分)，FTP 服务器的端口(4 分)，vsftp 服务(7 分)</td><td></td><td></td><td></td><td>FTP 服务器的配置过程(11 分)，测试 FTP 服务器配置成功情况(4 分)</td></tr>
<tr><td>2.5 Web 服务器的配置</td><td>Apache 服务器的配置(15 分)</td><td></td><td>Apache 服务器的配置(15 分)</td><td></td><td>Web 服务器的配置过程(15 分)，Apache 服务器的配置(15 分)</td><td></td><td></td><td>Web 服务器的功能(2 分)</td></tr>
<tr><td>2.6 代理服务器的配置</td><td></td><td>Linux 网卡的配置过程(15 分)</td><td></td><td></td><td>代理服务器软件(2 分)，代理服务器的配置过程(13 分)</td><td></td><td></td><td></td></tr>
<tr><td>2.7 DHCP 服务器的配置</td><td></td><td></td><td>DHCP 服务的工作过程(4 分)，DHCPServer 配置属性参数(7 分)</td><td></td><td></td><td></td><td>DHCP 工作流程(6 分)，DHCP Server 配置属性参数(4 分)，设置 Internet 协议属性参数(1 分)，PCI 重新租用 IP 地址的命令(4 分)</td><td></td></tr>
</table>

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2006.05	2006.11	2007.05	2007.11	2008.05	2008.11	2009.05	2009.11			
第3章网络安全设置	3.1 网络病毒防护策略和入侵处理策略		木马程序的特点(4分)，入侵处理策略(6分)，网络病毒防护策略(3分)							**1. 未变动的大纲要求：** ①防火墙的配置策略； ②入侵处理策略； ③漏洞处理策略； ④病毒及病毒防范。 **2. 新增的大纲要求：** ★DES和RSA的基本概念； ★认证； ★数字证书； ★安全电子邮件； ★HTTPS。 **3. 对大纲变化的说明：** 新增的大纲要求属于“加密、认证、数字签名等安全技术”。随着加密、认证、数字签名技术的广泛流行，安全技术被列入考试大纲。考生应充分引起注意。而原先的“网络病毒防范策略”被修改为“病毒及病毒防范策略”，只属于大纲叙述性的调整。	**1. 考题分布：** 通常出现在网络管理员考试(下午科目)的第4题。 **2. 阅读提示：** 本章对应教程“7.1 网络安全基础”、“7.2 防火墙”、“7.3 入侵检测”、“7.4 漏洞扫描”和“7.5 网络防病毒系统”。考生可以对照教程相关内容进行同步复习。 **3. 补充说明：** 教程内容已经基本覆盖大纲要求的考点，但需要注意的是增加了大纲未明确指出、教程未提及，但考试中遇到的重要考点。 ※访问控制列表； ※SSL与TCP/IP协议之间的关系。	本章节考点分值约占总考分的15%。考查针对一个网络环境来部署防火墙，如在网络中防火墙的连接位置、网络中不同部分的IP地址的配置等。并考查配置防火墙的规则(如源和目标的IP地址、通信协议、通信端口、数据传输的方向、通信允许或拒绝等)。高频考点为： ◆网络病毒的防护策略； ◆网络病毒的特点； ◆入侵处理策略； ◆防火墙的基本配置； ◆访问控制列表； ◆漏洞处理策略。
	3.2 防火墙的配置策略和漏洞处理策略		防火墙的功能(2分)	防火墙的类型和基本结构(3分)，防火墙内部的连接方式和设备(3分)，防火墙的功能(3分)，防火墙访问控制规则的配置(4分)，防火墙的地址隐藏功能配置(2分)	HTTPS的概念(2分)，SSL(13分)	防火墙的安全区域(4分)，防火墙访问控制规则的配置(11分)		防火墙的安全区域(2分)，包过滤防火墙的功能(2分)，ACL语句(8分)，防火墙的配置过程(3分)	配置NAT/基本防火墙的过程(15分)，防火墙的安全区域(4分)			
第4章网络管理与故障处理	4.1 网络管理软件	常见网络管理命令(7分)	常见网络管理命令(6分)	常用网络管理命令(4分)				常用网络管理命令(13分)	常用网络管理命令(2分)，常用网络管理命令(2分)	**1. 未变动的大纲要求：** ①使用网络管理软件对网络的配置、安全、性能、故障、计费进行监督和管理； ②简单网络故障的分析、定位、诊断和排除； ③小型网络的维护策略、计划和实施； ④数据备份和数据恢复； ⑤系统性能分析。 **2. 删除的大纲要求：** 系统潜在问题分析。 **3. 对大纲变化的说明：** “系统潜在的问题分析”属于多年命题中未曾考到的内容，大纲将其丢弃。此部分考查很灵活。要求考生具有处理实际问题的能力。	**1. 考题分布：** 通常出现在网络管理员考试(下午科目)的第3题，也偶尔出现在第1题。 **2. 阅读提示：** 本章对应教程的“8.1 网络管理简介”、“8.2 简单网络管理协议”、“8.3 网络管理工具”和“8.4 基于Windows的网络管理”。考生可以对照教程相关内容进行同步复习。	本章节考点分值约占总考分的10%。根据相关的故障现象来判断故障原因并排除故障。高频考点为： ◆常见的网络管理命令格式； ◆常用故障排除的方法； ◆网络故障的诊断。
	4.2 网络故障	网络故障诊断(2分)	常见的网络故障诊断(4分)，SNMP服务知识(15分)					网络故障排除(4分)，常见网络故障的排除(2分)	Web故障排除(2分)，网络病毒故障诊断(3分)，代理服务器故障诊断(2分)			

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2006.05	2006.11	2007.05	2007.11	2008.05	2008.11	2009.05	2009.11			
第5章 Web网站建设	5.1 用HTML制作网页	相关考题一般结合“5.2 动态网页制作”一起考。								**1. 未变动的大纲要求：** ①Web网站的规划、建设、管理与维护； ②HTML网页设计与制作； ③JSP、ASP动态网页编程技术。 **2. 新增的大纲要求：** ADO的概念和使用。 **3. 删除的大纲要求：** XML动态网页编程技术的基本概念。 **4. 对大纲变化的说明：** “ADO的概念”在往年的考题中已经隐含出现，即数据库的连接，大纲对该考点的增加，只是对该考点的明确化。“XML动态网页编程技术”在下午科目的考试中未曾出现过，现在大纲将其删除也是合理的。	**1. 考题分布：** 固定出现在网络管理员考试(下午科目)的第5题。 **2. 阅读提示：** 本章对应教程的“6.1 使用HTML制作网页”、“6.2 网页制作工具”、“6.3 动态网页的制作”以及“6.5 Web网站创建与维护”。考生可以对照教程相关内容进行同步复习。	本章节考点分值约占总考分的20%，考生应充分重视本章的复习。通常以程序填空的形式来完成具有指定功能的网页。高频考点为： ◆HTML常用元素； ◆ASP内嵌对象。
	5.2 动态网页制作	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)	ASP动态网页制作基础知识(15分)			
	5.3 Web网站的创建与维护	相关考题一般结合“5.1 用HTML制作网页”和“5.2 动态网页制作”一起考。										

目　　录

第 1 章　小型局域网的构建与综合布线

大纲要求：

- 小型计算机局域网的构建，包括网络规划、组网技术选择、组网设备选择及部署、设备配置和管理、划分 VLAN、综合布线系统。
- 交换机和路由器的基本配置，包括命令行接口访问交换机和路由器、Web 方式访问交换机和路由器、VLAN 配置、路由器路由协议配置、广域联网。

1.1　局域网组网的设计

1.1.1　考点辅导

1.1.1.1　局域网的设计原则

设计局域网时，应遵循以下原则。

1. 实用性原则

网络系统应采用成熟可靠的技术和设备，这样才能做到实用、经济和有效。

2. 开放性原则

网络系统应采用开放的标准和技术。

3. 可靠性原则

网络系统应确保很高的可靠性，具有较高的平均无故障时间和较低的平均故障率。

4. 安全性原则

网络系统应具有良好的安全性，以确保网络系统和数据的安全运行。

5. 先进性原则

网络系统应采用先进的技术和设备，以符合网络未来发展的潮流。

6. 高效性原则

网络系统应具有很高的资源利用率。

7. 可扩展性原则

网络系统应在规模和性能两方面具有良好的可扩展性。

8. 高性价比原则

网络系统应具有较高的性价比，技术优先，兼顾价格。

1.1.1.2 局域网的设计步骤

1. 网络需求分析

在组建局域网之前首先要进行需求分析工作，根据用户提出的要求，进行网络设计。网络建设的成败很大一部分取决于网络实施前的规划工作。

1) 网络的功能要求

任何网络都不可能是一个能够满足各项功能需求的“万能网”。因此，必须针对每个具体的网络所要完成的功能，依据使用需求、实现成本、未来发展、总预算投资等因素对网络的组建方案进行认真的设计和推敲。

2) 网络的性能要求

对网络系统处理的性能进行分析，根据网络的工作站权限、容错程度、网络安全性方面等要求，确定采取何种措施及方案。

3) 网络运行环境的要求

根据整个局域网运行时所需要的环境要求，确定使用哪种网络操作系统、应用软件和共享资源。

4) 网络的可扩充性和可维护性要求

如何增加工作站、怎样与其他网络联网、对软件/硬件的升级换代有何要求与限制等，都要在网络设计时加以考虑，以保证网络的可扩充性和可维护性。

2. 确定网络类型和带宽

与其他网络技术相比，以太网具有价格低、可靠性高、可扩展性好、易于管理等优点。所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备，目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或网络数据流量比较大的情况下，应采用千兆以太网技术，以满足对网络主干数据流量的要求。网络主干和分支方案确定以后，就可以选择集线器或交换机产品了。集线器或交换机的型号与数量由联入网络的计算机数量和网络拓扑结构来决定。

3. 确定网络设备

网络设备的选择应遵循以下原则。

1) 厂商的选择

所有网络设备尽可能选取同一厂家的产品，这样在设备的可互连性、协议互操作性、技术支持、价格等方面更有优势。

2) 扩展性考虑

在网络的层次结构中，主干设备应预留一定的扩展能力，而低端设备则够用即可，因为低端设备更新较快，且易于扩展。

3) 根据方案实际需要选型

在参照整体网络设计要求的基础上，根据网络实际带宽性能需求、端口类型和端口密度选择。如果是旧网改造项目，则应尽可能保留并延长用户对原有网络设备的投资，减少在资金投入方面的浪费。

4)　选择性价比高、质量过硬的产品

为了使资金的投入与产出能达到最大值，能以较低的成本、较少的人员投入来维护系统运转，网络开通后，能运行许多关键业务，要求系统具有较高的可靠性。

4. 确定布线方案和布线产品

现在的布线系统主要是光纤和非屏蔽双绞线，小型网络多以超五类非屏蔽双绞线为布线系统，因为布线是一次性工程，因此应考虑在未来几年内网络扩展的最大点数。

5. 确定服务器和网络操作系统

服务器是网络数据储存的仓库，其重要性可想而知。服务器的类型和档次应与网络的规模、数据流量以及可靠性要求相匹配。

如果是几十台计算机以下的小型网络，并且数据流量不大，选用入门级服务器基本上可以满足需要；如果是数百台左右的中型网络，则应选用工作组级服务器；如果是上千台的大型网络，则应选用企业级服务器。

服务器的数量由网络应用来决定，可以根据实际情况，配备 E-mail 服务器、Web 服务器、数据库服务器等，也可以让一台服务器充当多种服务器角色。

目前，网络操作系统基本上是三分天下：微软的 Windows 2000 Server、传统的 UNIX 和 Linux，可以根据网络规模、技术人员水平、资金等综合因素来决定究竟使用什么网络操作系统。

6. 其他

局域网的设计还包括不间断电源、网络安全、互联网接入、网络应用系统等方面的设计。

1.1.2　典型例题分析

例 1　请简要回答如下局域网设计时的有关问题。

【问题 1】简述设计网络系统时需遵循的基本原则。

【问题 2】局域网的硬件设备目前大多选择什么网络设备？

【问题 3】以太网的特点是什么？

【问题 4】局域网设计与连接时考虑的主要因素是什么？

分析：设计局域网时，应遵循以下原则：实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则和高性价比原则。

以太网技术是目前局域网技术中最成熟的技术。所以局域网的硬件设备大多选择以太网的网络设备。以太网的特点如下。

(1)　开放标准，获得众多厂商的支持。目前，几乎所有的硬件制造商生产的设备和几乎所有的软件开发商的操作系统和应用协议都与以太网兼容。

(2)　易于移植和升级，可最大限度地保护用户投资。对于所有以太网技术，其帧的结

构几乎是一样的，这就提供了非常好的升级途径。快速以太网技术提供了从 10Mb/s 向 100Mb/s 以太网的平滑升级。千兆和万兆以太网的出现，在增加带宽的同时也扩展了可升级性。只要将低速以太网设备用交换机连接到千兆或万兆以太网的设备上，就可实现一个物理线速向另一物理线速的适配。这样的升级方式就使得千兆和万兆以太网能无缝地与现在的以太网集成在一起。

(3) 价格便宜，管理成本低。以太网技术在价格上与其他技术相比具有优越性。若全面采用以太网解决方案，价格将更具有吸引力。另外，以太网存在时间长，标准化程度高，一般网络管理人员都比较熟悉，因此它的运行维护管理成本也比较低。

(4) 结构简单，组网方便。以太网技术的实现原理统一采用了 CSMA/CD 媒体访问控制方法，不同版本的以太网的帧结构和网络拓扑结构也是一致的，对布线系统的要求较低，网络连接设备的配置比较简单。

所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备，目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或在网络数据流量比较大的情况下，应采用千兆以太网技术，以满足对网络主干数据流量的要求。网络主干和分支方案确定之后，就可以选定集线器或交换机产品了。集线器或交换机的数量由联入网络的计算机数量和网络拓扑结构来决定。

答案：

【问题 1】设计网络系统时应遵循：实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则、高性价比原则。

【问题 2】以太网。

【问题 3】以太网具有开放标准，获得众多厂商的支持；易于移植和升级，最大限度地保护用户投资；价格便宜，管理成本低；结构简单，组网方便等特点。

【问题 4】网络类型和带宽。

1.1.3 同步练习

如何确定局域网的服务器？局域网常使用的操作系统有哪些？

1.1.4 同步练习参考答案

服务器是网络数据储存的仓库，其重要性可想而知。服务器的类型和档次应与网络的规模和数据流量以及可靠性要求相匹配。如果是几十台计算机以下的小型网络，而且数据流量不大，选用入门级服务器基本上可以满足需要；如果是数百台左右的中型网络，选用工作组服务器；如果是上千台的大型网络，选用企业级服务器。

局域网常使用的操作系统有微软的 Windows 2000 Server、UNIX 和 Linux。

1.2　局域网组网技术及设备选择

1.2.1　考点辅导

1.2.1.1　局域网基础

1. 局域网参考模型

局域网体系结构由物理层、媒体访问控制子层(MAC)和逻辑链路控制子层(LLC)组成。

IEEE 802 参考模型的最底层对应于 OSI 模型中的物理层，具体包括以下功能。

(1) 信号的编码/解码。

(2) 前导码的生成/去除(前导码仅用于接收同步)。

(3) 位的发送/接收。

IEEE 802 参考模型的 MAC 子层和 LLC 子层合起来与 OSI 模型中的数据链路层相对应。MAC 子层完成的功能如下。

(1) 在发送时将要发送的数据帧组装成帧，帧中包含地址和差错检测等字段。

(2) 在接收时，将接收到的帧解包，并进行地址识别和差错检测。

(3) 管理和控制对于局域网的传输媒体的访问。

LLC 子层完成的功能如下。

(1) 为高层协议提供相应的接口，即一个或多个服务访问点(SAP)，通过 SAP 支持面向连接的服务和复用能力。

(2) 端到端的差错控制和确认，确保无差错传输。

(3) 端到端的流量控制。

需要指出的是，在局域网中采用了两级寻址，用 MAC 地址标识局域网中的一个站，LLC 提供了服务访问点地址，SAP 指定了运行于一台计算机或网络设备上的一个或多个应用进程地址。

2. 局域网拓扑结构

按照不同的物理布局，局域网的拓扑结构通常可分为 3 种，分别是总线型拓扑结构、星型拓扑结构和环型拓扑结构。

总线型结构是使用同一媒体或电缆连接所有端用户的一种方式，也就是说，连接端用户的物理媒体由所有设备共享。

星型结构有中心节点，各节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中心节点来转接。

环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户连接到另一个端用户，直到将所有端用户连成环型。

3. 局域网媒体访问控制方法

目前，计算机局域网常用的访问控制方式有 3 种，分别是载波侦听多路访问/冲突检

测(CSMA/CD)、令牌环访问控制法(Token Ring)和令牌总线访问控制法(Token Bus)。

CSMA/CD 包含两方面内容，即载波侦听(CSMA)和冲突检测(CD)。CSMA/CD 访问控制方式主要用于总线型网络拓扑结构，是 IEEE 802.3 局域网标准的主要内容。

Token Ring 是令牌通行环的简写。其主要技术指标是：网络拓扑为环型布局，基带网，数据传送速率为 4Mb/s，采用单个令牌(或双令牌)的令牌传递方法。环型网络的主要特点是：只有一条环路，信息单向沿环流动，无路径选择问题。

Token Bus 是令牌通行总线(Token Passing Bus)的简写。这种方式主要用于总线型或树型网络结构中。1976 年美国 Data Point 公司研制成功的 ARCnet(Attached Resource Computer network)网络综合了令牌传递方式和总线网络的优点，在物理总线结构中实现令牌传递控制方法，从而构成一个逻辑环路。此方式也是目前计算机局域网中的主流介质访问控制方式。

1.2.1.2 无线局域网简介

1. 无线数据网络的种类

无线数据网络解决方案包括无线个人网、无线局域网、无线城域网和无线广域网。

无线个人网主要用于个人用户工作空间，典型的覆盖距离为几米，可与计算机同步传输文件，访问本地外围设备，通常被形容为满足“最后 10 米”的通信需求，目前的主要技术为蓝牙(Bluetooth)技术。

无线局域网(Wireless LAH，WLAH)是一种借助于无线技术取代有线布线方式构成局域网的新手段。WLAN 可提供传统有线局域网的所有功能，是计算机网络与无线通信技术相结合的产物。目前，WLAN 领域主要是 IEEE 802.11x 标准系列，其中应用最为广泛的是 IEEE 802.11b。

无线城域网是一种有效作用距离比 WLAN 更远的宽带无线接入网络，通常用于城市范围内的业务点和信息汇聚点之间的信息交流和网际接入。有效覆盖区域为 2～10km，最大可达 30km，数据传输率最快可达 70Mb/s，目前的主要技术标准是 IEEE 802.16 系列。

无线广域网(Wireless WAN，WWAN)主要用于满足一个城市范围的信息交流的无线接入需求。IEEE 802.20 和 3G 蜂窝移动通信系统是 WWAN 的主要标准。

2. 无线局域网的扩频技术

无线局域网采用电磁波作为载体传送数据信息，使用的模式主要是窄带和扩频。目前，无线局域网的数据传输通常采用无线扩频技术(Spread Spectrum，SST)。常见的扩频技术包括两种：跳频扩频(Frequency-Hopping Spread Spectrum，FHSS)和直接序列扩频(Direct Sequence Spread Spectrum，DSSS)，它们都工作在 ISM 频段(Industrial Scientific Medical Band，ISM)上。

3. 无线局域网的拓扑结构

无线局域网分为对等网络和结构化网络两种拓扑结构。

对等网络(Peer to Peer)用于一台计算机(无线工作站)和另一台或多台计算机(其他无线工作站)之间的直接通信，该网络无法接入有线网络中，只能独立使用。对等网络中的一个节点必须能“看”到网络中的其他节点，否则就认为网络中断。因此对等网络只适应于少数用户的组网环境，并且距离足够近。

结构化网络(Infrastructure)由无线访问点(Access Point，AP)、无线工作站(Station，STA)以及分布式系统(DSS)构成，覆盖的区域分为基本服务区(Basic Service Set，BSS)和扩展服务区(Extended Service Set，ESS)。

4. 无线局域网的主要工作过程

无线局域网的主要工作过程包括：扫频、关联、重关联和漫游。

5. 无线局域网的访问控制方式

IEEE 802.11b 标准的无线局域网使用的是带冲突避免的载波侦听多路访问方法(CSMA/CA)。

1.2.1.3　10Mb/s 以太网

10Mb/s 以太网一般指速率小于或等于 10Mb/s 的低速以太网。根据传输介质的不同，10Mb/s 以太网大致有 4 个标准，各个标准的 MAC 子层媒体访问控制方法和帧结构以及物理层的编码方法(曼彻斯特编码)均是相同的，不同的是传输媒体和物理层的收发器及媒体连接方式，按照技术出现的时间顺序，这 4 个标准依次如下。

1. 粗缆以太网(10Base5)

10Base5 采用 RG-11 型粗同轴电缆为传输介质，其阻抗为 50Ω，直径为 0.4in。在 10Base5 中，每个计算机节点都通过网卡(AUI 接口)、收发器电缆(AUI Cable)和“收发器”与总线相连，如图 1-1 所示。

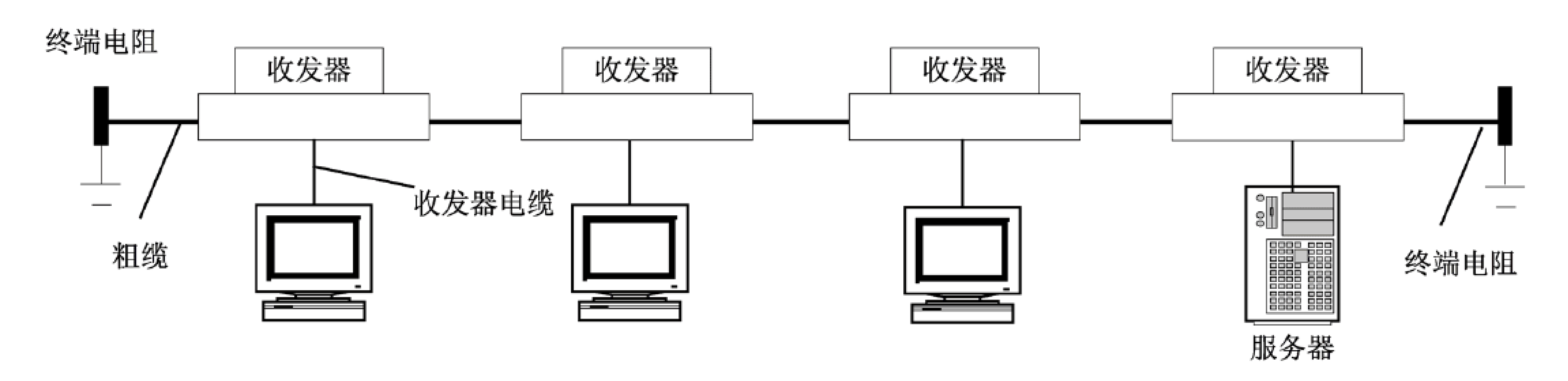


图 1-1　10Base5 网络结构

10Base5 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，每一个网段最长为 500m。

通常在标准以太网网络接口板上提供一个 15 针的 AUI(DIX)接口，收发器电缆采用 78Ω 的 6 对屏蔽双绞线电缆(STP)，将收发器与 PC 网卡连接，粗同轴电缆两端接上 50Ω 的终端匹配器(也称端接器)，其中之一必须接地，这就构成了网络段，每段最远距离为 500m。一个粗缆以太网最多可以有 5 段。电缆最大距离是 2.5km，工作站之间的最小距离为 2.5m，收发器电缆的最长距离为 50m。

1) 硬件基本配置

网卡：联网的每个节点都需要一块带有 15 针 AUI(DIX)接口的 10Mb/s 网卡。

收发器：粗缆以太网的每个节点需要通过一个安装在总线同轴电缆上的外部收发器(带有 15 针的 AUI 接口)连入网内。

收发器同轴电缆(AUI 电缆)：用于节点中网卡与收发器的连接。

电缆系统：RG-11 型 50Ω 粗同轴电缆，终端电阻安装在电缆的两端，防止信号的反射，其中之一必须接地。

中继器：主要用来扩展作为总线的同轴电缆长度和工作站(节点)个数。

2) 主要技术参数

在粗缆以太网中，不使用中继器时，每段粗缆的最大距离为 500m。如果使用中继器，应遵循 5-4-3 规则，即一个粗缆以太网中最多允许使用 4 个中继器，连接 5 段最大长度为 500m 的粗同轴电缆；而 5 段中只有 3 段可以连接工作节点，其余两段只能用于扩展网络距离。使用中继器后的粗缆以太网的最大长度不能超过 2.5km；由于每个以太网段中连入的节点数最多为 100 个，最多可以有 3 个网段连接工作节点，因此，最多有 300 个工作节点；两个相邻的收发器之间的最小距离为 2.5m，收发器电缆的最大长度为 50m。

3) 特点

优点：可靠性高，抗干扰能力强，作用距离长。

缺点：粗缆较贵，而且要求每个工作站都配置一个外部收发器和收发器电缆，因而成本较高、网络投资较大。

4) 主要技术规范

拓扑结构：总线。

介质访问控制方法：CSMA/CD。

网络类型：RG-11 型 50Ω 粗同轴电缆。

传输速度：10Mb/s。

最大网络节点数目：300 个。

每段最大节点数目：100 个。

最大网段数目：5 个，最多使用 4 个中继器，其中 3 个网段可连接工作节点。

节点间的最小距离：2.5m。

最大网络长度：2.5km。

最大网段长度：500m。

2. 细缆以太网(10Base2)

10Base2 使用 RG-58 型细缆、BNC-T 型连接器，以线性总线进行布线。10Base2 将原来 10Base5 的收发器功能移植到网卡上，因此，使得网络的组建更简单，性价比也比 10Base5 高，然而，却也因此限制了信号能够传送的最大距离。其结构如图 1-2 所示。

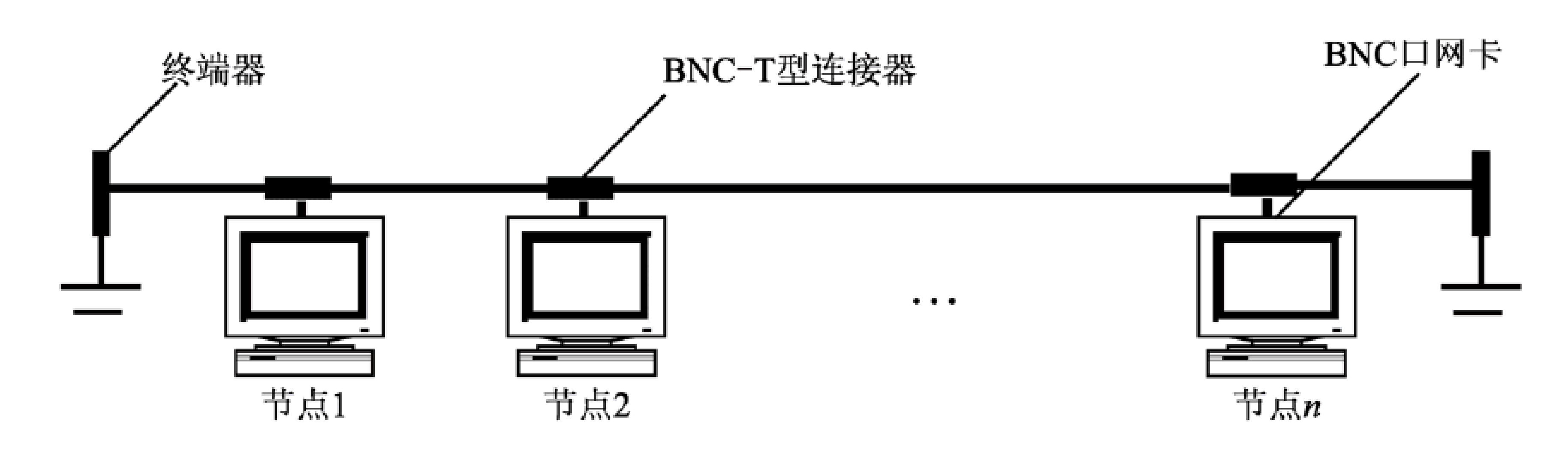


图 1-2 10Base2 网络结构

10Base2 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，每一个网段最长约

为 200m。

一个细缆以太网的“单段”最大长度为 185m，最多可使用 4 个中继器，即可以有 5 个电缆段，而 5 段中只有 3 段可以连接工作节点，其余两段只能用于扩展网络距离。电缆总长度最大为 925m。一个网段中节点的最多数目为 30 个，因此，最多可以有 90 个工作节点。

两个相邻的 BNC-T 型连接器的最小距离为 0.5m，每段的两端都必须安装一个 50Ω 终端匹配器，并且其中一端应接地。网卡提供 BNC 接口，同轴细缆通过 T 型接头与网卡连接，所有 T 型接头必须直接接到工作站 BNC 接口上，中间不得接入任何电缆。

如图 1-3 所示为一个使用中继器扩展网络距离的双网段 10Base2 组网实例。

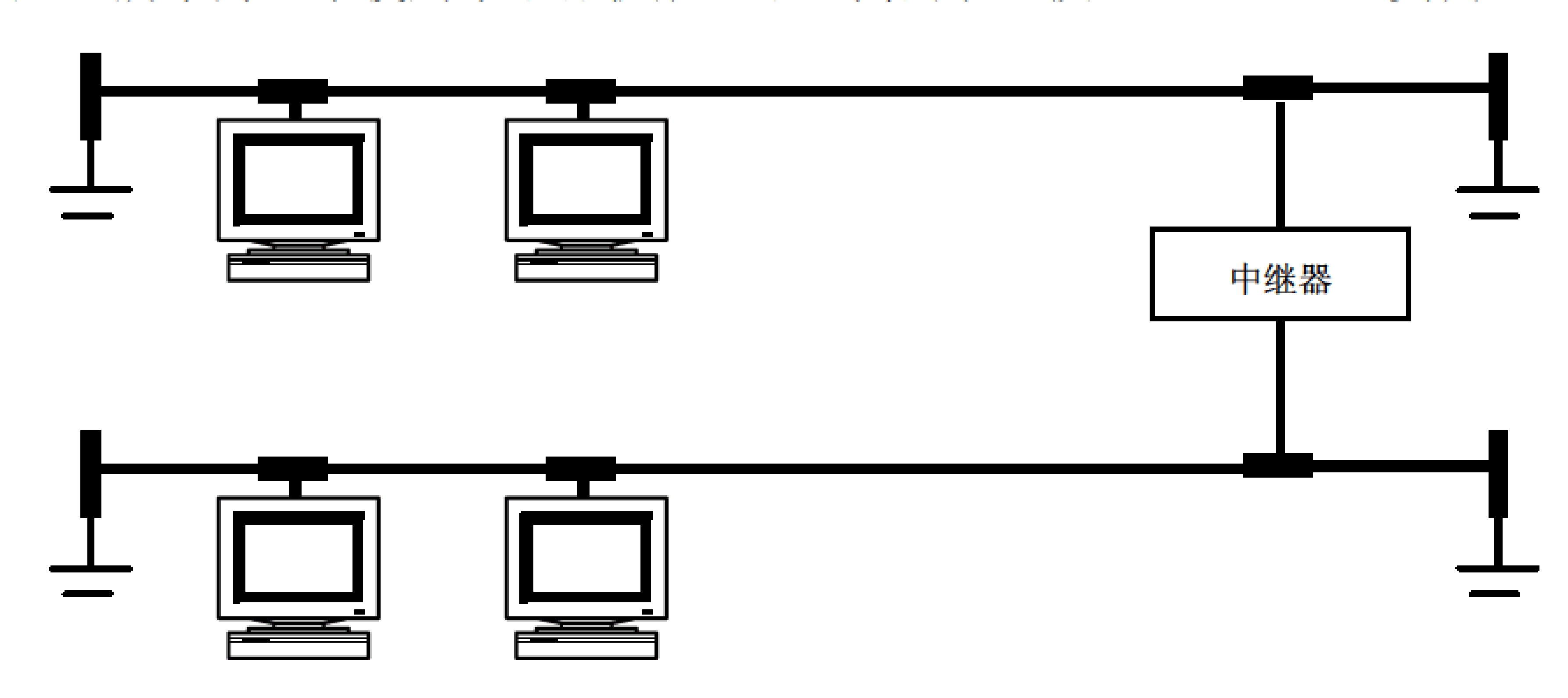


图 1-3　使用中继器连接的双网段 10Base2 网络结构

1)　硬件基本配置

网卡：带有 BNC 接口的 10Mb/s 网卡。

BNC-T 型连接器：细缆以太网中的每个节点通过 BNC-T 型连接器连入网内。

电缆系统：RG-58 型 50Ω 细同轴电缆，终端电阻安装在电缆的两端，防止信号的反射，其中之一必须接地。

中继器：主要用来扩展作为总线的细轴电缆长度和工作站(节点)个数。

2)　特点

优点：系统造价低廉，安装容易，具有最短的布线距离。

缺点：由于缆段中联入多个 BNC-T 型连接器，存在着多个 BNC 型连接头和 BNC-T 型连接器的连接点，因而同轴电缆连接的故障率较高。

3)　技术规范

拓扑结构：总线。

介质访问控制方法：CSMA/CD。

网络类型：RG-58 型 50Ω 细同轴电缆。

传输速度：10Mb/s。

最大网络节点数目：90 个。

每段最大节点数目：30 个。

最大网段数目：5 个，最多使用 4 个中继器，其中 3 个网段可以连接工作节点。

节点间的最小距离：0.5m。

最大网络长度：925m。

最大网段长度：185m。

3. 双绞线以太网(10BaseT)

10BaseT 以太网是使用非屏蔽双绞线(UTP)电缆来连接的传输速率为 10Mb/s 的以太网。10BaseT 以太网支持结构化布线系统，需要使用集线器(Hub)构成总线型和星型结合的混合型网络拓扑，具有良好的故障隔离功能，使得网络任一段线路或任一工作站点出现障碍时，均不影响网络上的其他站点，简化了网络故障诊断过程，缩短了故障诊断时间，提高了网络故障检测和冲突控制效率，使局域网难于维护的缺点得以根本性改变。加之其组网容易，使得 10BaseT 以太网成为目前使用最广的局域网系统。

10BaseT 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，T 表示的是传输媒体双绞线。

单个集线器和多个集线器的 10BaseT 以太网连接如图 1-4 所示。

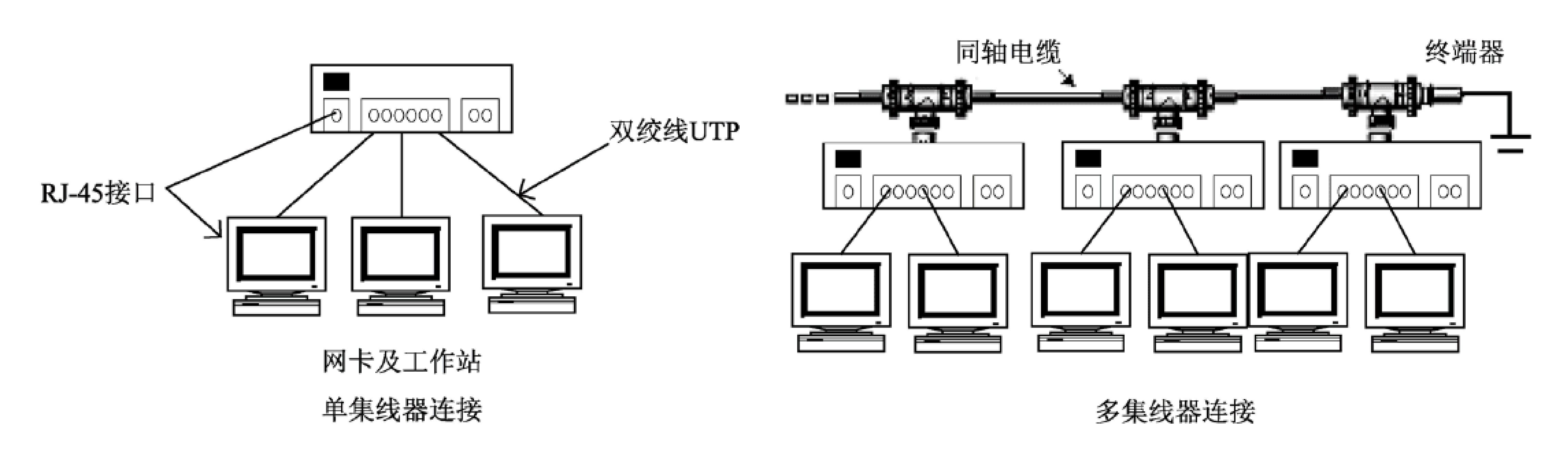


图 1-4　10BaseT 以太网连接

1)　硬件基本配置

集线器：即 Hub，是双绞线以太网的中心连接设备，有多个 RJ-45 型接口，能支持多个工作站(客户机)入网。Hub 上的 RJ-45(级联或普通)接口还可以与其他 Hub 相连，易于扩展网络。Hub 上的 BNC 向上接口与 BNC-T 型连接器相接时，可以与细缆以太网相连。Hub 上的 AUI 接口可以与粗缆以太网的收发器电缆相连。新型的高速 Hub 上还配有光纤接口，通过此接口，可以接入光纤主干线。

非屏蔽双绞线：10BaseT 网络标准最低采用 3 类 UTP，两端都装有同样的 RJ-45 型接头(水晶头)，每一个工作节点都需要一根双绞线电缆，用来连接工作节点上的网卡与集线器。

网卡：带有 RJ-45 接口的网卡。

2)　扩展组网方案

使用集线器和双绞线的以太网结构分为：单集线器结构、多集线器级联结构、叠加集线器结构。

(1)　多集线器级联(Uplink)结构。

对于规模较大，或节点(工作站)数超过单集线器的端口数目，常采用多集线器的连接，这就是集线器的“级联”。级联的目的是为了组成更大规模的网络，级联结构的 10BaseT 网络也遵循 5-4-3 规则，即任一条通路上的两台计算机之间最多不能超过 5 段线，即最多可以串联 4 个集线器；这段线既包括集线器与集线器的连线，也包括集线器到计算机间的连线。注意：3 个集线器能连接设备，两个只能用于级联。网络上连接设备的总数不得超过

1024 台。在级联之前，必须首先弄清集线器上的端口类型。

普通集线器提供的端口类型有以下 3 类。

- 用于连接节点(工作站或服务器)的普通 RJ-45 端口。
- 专门用于双绞线以太网集线器的级联端口。即专门用于级联的“出口/入口”，或者是 Uplink 端口。
- “向上连接端口”。这些端口可以连接粗缆的 AUI 端口，或细缆的 BNC 端口，也可以连接光纤端口。

(2) 对应于不同的端口，多集线器结构的级联有以下几种方法。

- 使用“标准线”，通过以太网集线器上专门的 RJ-45 型级联“出/入”端口进行级联。
- 对于没有专门级联“出口/入口”的两个集线器，可以使用“标准线”将一个集线器上边的 Uplink 端口与另一个集线器上边的普通 RJ-45 型端口相连，从而实现多集线器之间的级联。
- 使用“交叉线”连接两个没有“级联”口的集线器上的普通 RJ-45 接口，也可以实现多集器的级联。
- 使用同轴电缆、光纤，通过集线器提供的“向上连接端口”实现级联。

由于 10BaseT 以太网和粗、细缆以太网都属于 IEEE 802.3 规范，因此，互连十分方便。连接时，通常采用同轴电缆作为主干网，通过双绞线作为分支网络，这样可以提高干线的可靠性与干扰能力，并可延长传输距离。

利用集线器的“向上连接端口”进行级联，可以扩大局域网覆盖范围。例如，如果使用细缆连接两个集线器，细缆的单根缆段的最大长度为 185m，那么两个 10BaseT 网络中节点的最大距离可达到 385(185+100+100)m。如果使用粗缆连接两个集线器，粗缆的单根缆段的最大长度为 500m，那么网中两节点之间的最大距离可达到 700(500+100+100)m；如果在粗或细缆段中配合使用中继器，那么多缆段、多集线器级联系统的覆盖范围还可以更大。

(3) 可叠加集线器以太网结构。

可叠加集线器适用于中小企业联网环境。它由一个基础集线器与多个扩展集线器组成。基础集线器是一个具有网络管理功能的独立集线器。通过基础集线器，可以叠加多个扩展集线器，一方面可以增加以太网的节点(工作站)数目；另一方面可以实现对网络中工作节点的网络管理功能。其结构如图 1-5 所示。

3) 特点

(1) 优点

- 故障检测容易，当某一段线路、工作站或互连的某个 Hub 出现故障时，Hub 会将故障节点自动排除在网络之外，因而保证了剩余部分的正常工作。
- 安装、管理和使用都很简单，适于中小型单位自行组建局域网。
- 具有成本低、扩展方便、改变网络布局容易等优点。

(2) 缺点

- 这种结构的最大缺点在于它是一种共享介质的网络，随着网络节点的增加，冲突也会增加，网络的性能也会随之急剧下降。有实验表明，一个单 Hub 的 10BaseT，虽然具有 10Mb/s 的带宽，但是当网络工作节点增至 20 个的时候，其实际的可用

带宽将降至原来的 30%～40%。此外，当使用多个 Hub(最多 4 个)级联时，或者是与其他以太网连接之后，所有网络节点将共享 10Mb/s 的带宽。Hub 所连接的节点越多，每个工作节点得到的带宽就越窄。在高负荷时，网络性能将急剧下降，这是组建共享式以太网遇到的最大问题。

- 网络的中央节点的负荷过重，一旦 Hub 出现故障，将导致整段或全部网络瘫痪。
- 双绞线的抗干扰能力弱。
- 由于每个单段网线只能连接一个工作节点，所以网络通信线路的利用率很低。

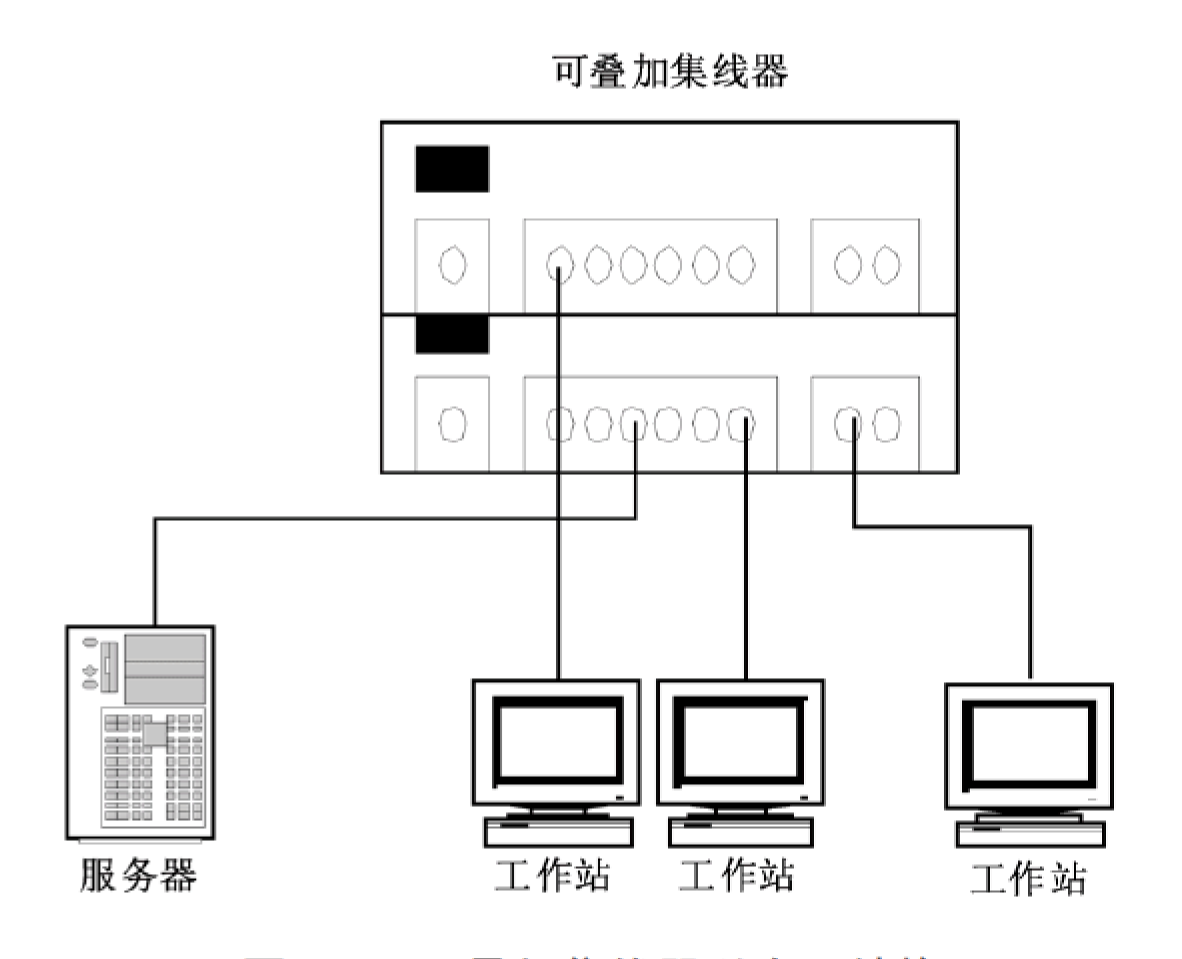


图 1-5　可叠加集线器以太网结构

4)　技术规范

拓扑结构：由于介质访问控制方法为 CSMA/CD，因此，10BaseT 是逻辑上的总线型拓扑结构，物理上的星型拓扑结构。

网线类型：3 类、5 类或超 5 类的非屏蔽双绞线。

传输速度：10Mb/s。

最大网络节点数目：1024 个。

每段最大集线器数量：1 个。

级联的最大集线器数量：4 个。

最大网络长度：500m。

最大网段长度：100m。

4.　光纤以太网(10BaseF)

10BaseF 以太网传输媒体采用多模光纤，拓扑结构为星型，所有站点连接到一个支持光纤接口的中心集线器上，每个电缆段的长度不能超过 2km。

10BaseF 以太网设计也遵循 5-4-3 法则，但由于受 CSMA/CD 碰撞域的影响，整个网络的最大跨距为 4000m。

10BaseF 代表的具体含义是：工作速率为 10Mb/s，采用基带信号，F 表示的是传输媒体光纤。

1.2.1.4　快速以太网

1. 快速以太网简介

快速以太网是在传统以太网的基础上发展而来的，因此它不仅保持相同的以太网帧格式，而且还保留了用于以太网的 CSMA/CD 媒体访问控制方式。由于快速以太网的速率比普通以太网提高了 10 倍，所以快速以太网中的网桥、路由器和交换机都与普通以太网不同，它们具有更快的速率和更短的延时。

目前，正式的 100BaseT 标准定义了 3 种物理层规范以支持不同的物理介质，具体如下。

(1) 100BaseTX 用于两对 5 类 UTP 或 1 类 STP。

(2) 100BaseT4 用于四对 3 类、4 类或 5 类 UTP。

(3) 100BaseFX 用于光纤。

其中，100BaseTX 规范描述如何通过 1 类屏蔽双绞线或者 5 类非屏蔽双绞线传送快速以太网帧。5 类 UTP 是目前使用最为广泛的介质，100BaseTX 标准使用其中两对，连接方法和 10BaseT 完全相同，其采用的拓扑结构为星型。这就意味着不必改变布线格局就可直接将 10BaseT 的布线系统移植到 100BaseTX 上。

100BaseT4 规范提出了 100BaseTX 在 3 类 UTP 上传送数据的具体规定，即 100BaseT4 使用四对 3 类、4 类或 5 类 UTP，连接最大距离为 100m。而 10BaseT 只使用两对线，因此老式的 3 类 UTP 布线的 10BaseT 系统必须改变端点上的电缆连线，才能正常运行 100BaseT4。

100BaseFX 是针对光纤提出的物理层规范，它的连线比 100BaseTX 长(450m)，如果采用非标准的全双工模式，连线长度可达 2km，单模光纤传输距离可达 40km。另外，抗干扰能力也大大优于 UTP 和 STP。

2. 100BaseT 组网方法

目前大部分以太网系统都配置一台或多台服务器，在采用以太网/快速以太网交换技术升级组网时，可以将原以太网服务器的网卡更换为快速以太网卡(100BaseTX 网卡)，并利用 5 类 UTP 通过 RJ-45 端子接入 100Mb/s 交换机的 100Mb/s 高速端口上。对于一般工作站，不必更换网卡，可通过原来的共享 Hub 集中连接到 100Mb/s 交换机级联的 10/100Mb/s 交换机的 10Mb/s 端口上，组成 10Mb/s 共享网。对于那些对带宽要求较高的数据库服务器，工作站以及打印机等，可单独连接到 10/100Mb/s 交换机的端口上，组成多级交换机的快速以太网。其连接方法如图 1-6 所示。

3. 快速以太网的拓扑结构

100BaseT 除了在传输介质、网卡、工作站、Hub 以及服务器硬件组成等方面与 10BaseT 相同外，还保持了 10BaseT 的网络拓扑结构，即所有站点都连接到集线器或交换机上，而集线器与站点间的最大距离仍为 100m。由于 100BaseT 对 MAC 子层的接口有所拓展，因此，快速以太网的拓扑结构形式也有相应的发展。

100BaseT 的拓扑规则如下。

(1) 最大 UTP 电缆长度为 100m。

(2) 在一条链路上，对于 I 类中继器(延时为 0.7μs 以下)，最多只能使用 1 个，可以构成每段长 100m 的两段链路，即站点到中继器距离为 100m，中继器到交换机距离为 100m。

对于Ⅱ类中继器(延时为 0.46μs 以下)，最多使用两个，可有每段长为 100m 的两段链路和 5m 长的中继器间链路，其中站点到第一个中继器(可用集线器)的距离为 100m，集线器与第二个中继器间的距离为 5m，第二个中继器到路由器或交换机的距离为 100m，站点到交换机的最大距离为 205m。

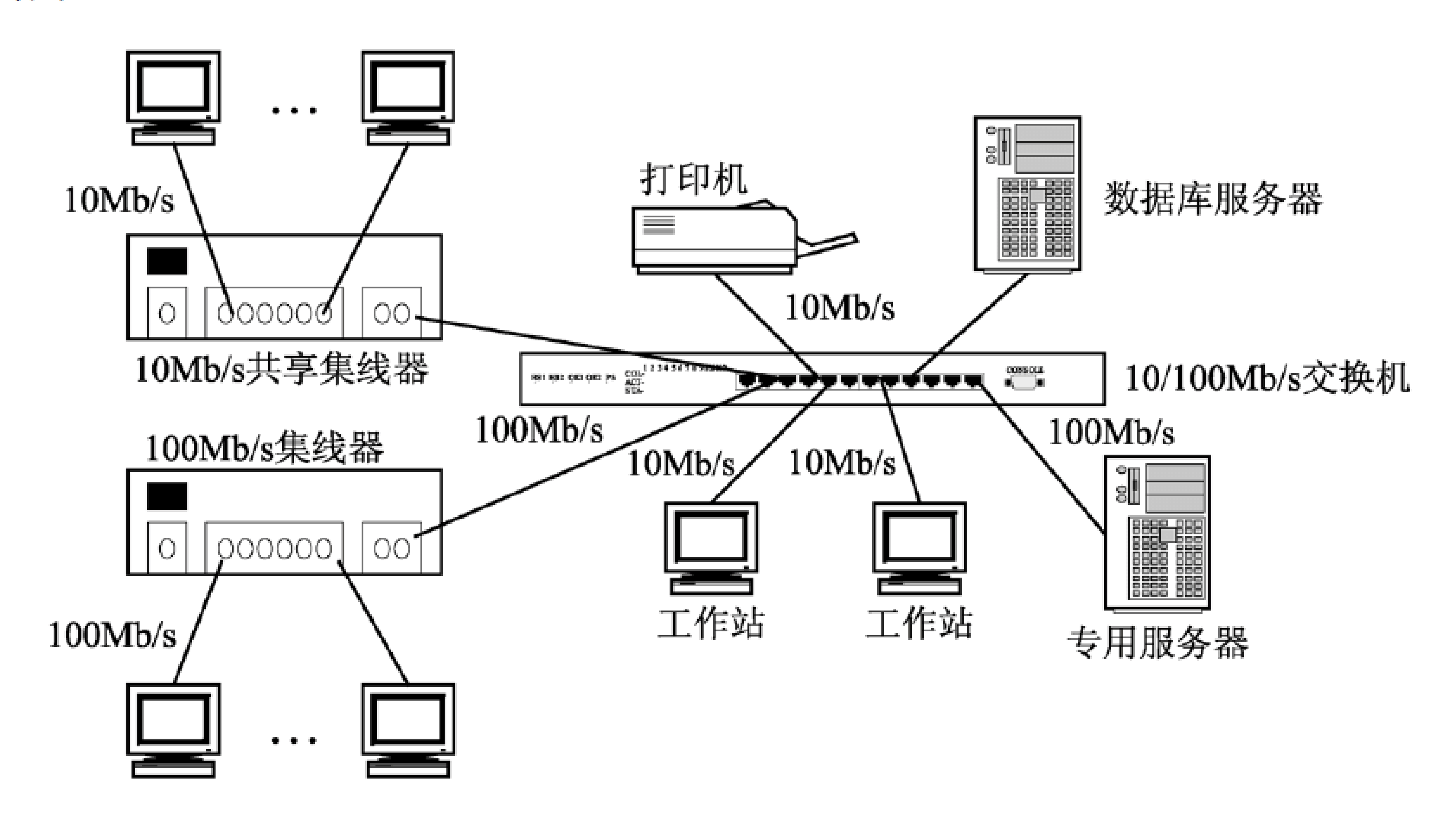


图 1-6　多级交换机快速以太网

(3) 对于光纤作为垂直布线的拓扑结构，纵向只能连接一个中继器(Hub)，各站点到 Hub 的最大距离为 100m，而 Hub 到交换机(或路由器)的垂直向下链路可采用 225m(最大限度)光纤，站点到交换机的最大距离为 325m。

(4) 利用全双工光纤的拓扑结构，通过非标准的 100BaseFX 接口连接，可以使站点(远程)或集线器到路由器或交换机的距离达到 2km。

根据上述规则构成的 100BaseT 拓扑结构如图 1-7 所示。将上述规则进行组合，利用光纤和交换机、网桥、路由器来连接主干设备、网段和工作站，可实现大型企业级和政府级网络。

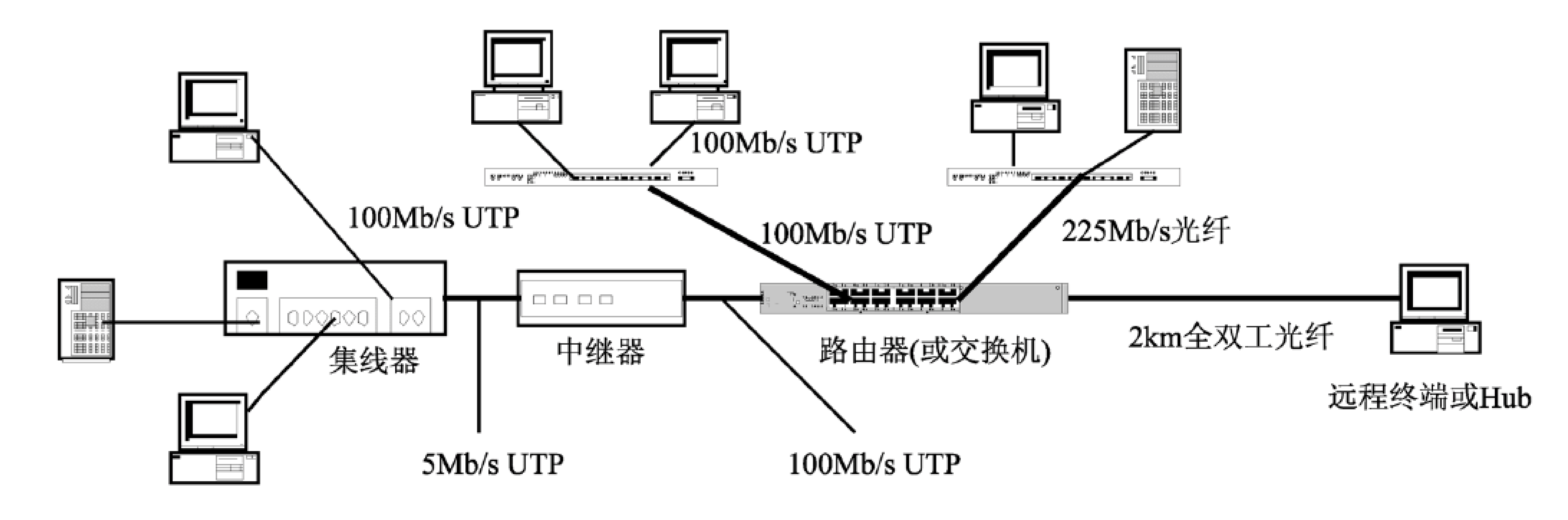


图 1-7　快速以太网的网络拓扑结构

1.2.1.5　千兆位以太网

千兆位以太网是 IEEE 802.3 标准的扩展，在保持与以太网和快速以太网设备兼容的同时，提供 1000Mb/s 的数据带宽。千兆位以太网为交换机到交换机和交换机到节点工作站的连接提供了新的全双工操作模式，还为采用中继器和 CSMA/CD 共享连接提供了半双工操

作模式。千兆位以太网与 IEEE 802.3 网络采用同样的帧格式、大小以及管理方式。它最初要求使用光纤电缆，但目前在 5 类非屏蔽双绞线电缆中也能很好地实现。

1. 千兆位以太网的分类

千兆位以太网根据传输介质的不同可以分为 4 种，如表 1-1 所示。

表 1-1　千兆位以太网的主要参数

千兆位以太网标准	传输介质	最大传输距离/m	
		半双工	全双工
1000BaseSX	62.5μm MMF	275	300
	50μm MMF	330	550
1000BaseLX	MMF	330	550
	SMF	330	5000
1000BaseCX	铜质屏蔽双绞线	25	25
1000BaseTX	超 5 类非屏蔽双绞线(4 对)	100	100

千兆位以太网标准只允许在媒体段中配置一个中继器，实际上在半双工模式下也只能配置一个中继器，增加一个中继器后，铜缆媒体的跨距会增大一倍，而光纤媒体的跨距反而会减少。其系统覆盖范围如下。

- 1000BaseLX/SX：240m。
- 1000BaseCX：50m。
- 1000BaseTX：200m。

2. 以太网向千兆位以太网的升级方法

现有以太网将逐渐向千兆位以太网升级，升级首先在现有的以太网 LAN 骨干网上进行，然后是服务器连接的升级，最终是工作站的升级。这些升级包括以下方面。

(1) 交换机到交换机链路的升级：快速以太网交换机或中继器之间的 100Mb/s 链路会被 1000Mb/s 的链路所替代，以提高骨干网交换机之间的通信速度，并支持更多的交换型和共享型快速以太网网段。

(2) 交换机到服务器链路的升级：在交换机和高性能服务器之间实现 1000Mb/s 链路的连接，并要求服务器安装千兆位以太网网卡。

(3) 快速以太网骨干网的升级：带有 10/100Mb/s 端口的快速以太网交换机可以升级支持多路 100/1000Mb/s 端口的千兆位以太网交换机或路由器和集线器(具有千兆位以太网接口和中继器)。这种升级允许服务器通过千兆位以太网网卡直接连接到骨干网上，可增加用户的高带宽应用与服务器的流量。千兆位以太网可以支持更多的网段、带宽和节点。

(4) 高性能工作站的升级：千兆位以太网网卡可将高性能工作站计算机升级到千兆位以太网。这些工作站计算机要连接到千兆位以太网的交换机或中继器上。

3. 千兆位以太网的应用

千兆位以太网可以用于布线间到网络核心的通信，如图 1-8 所示。如需要为个别用户提供 10Mb/s 或 100Mb/s 交换或组交换时，可以通过快速以太网连接，也可以通过千兆位以太

网链路连接。为了提高文件服务器的吞吐性能，它的连接也可以通过千兆位以太网进行。

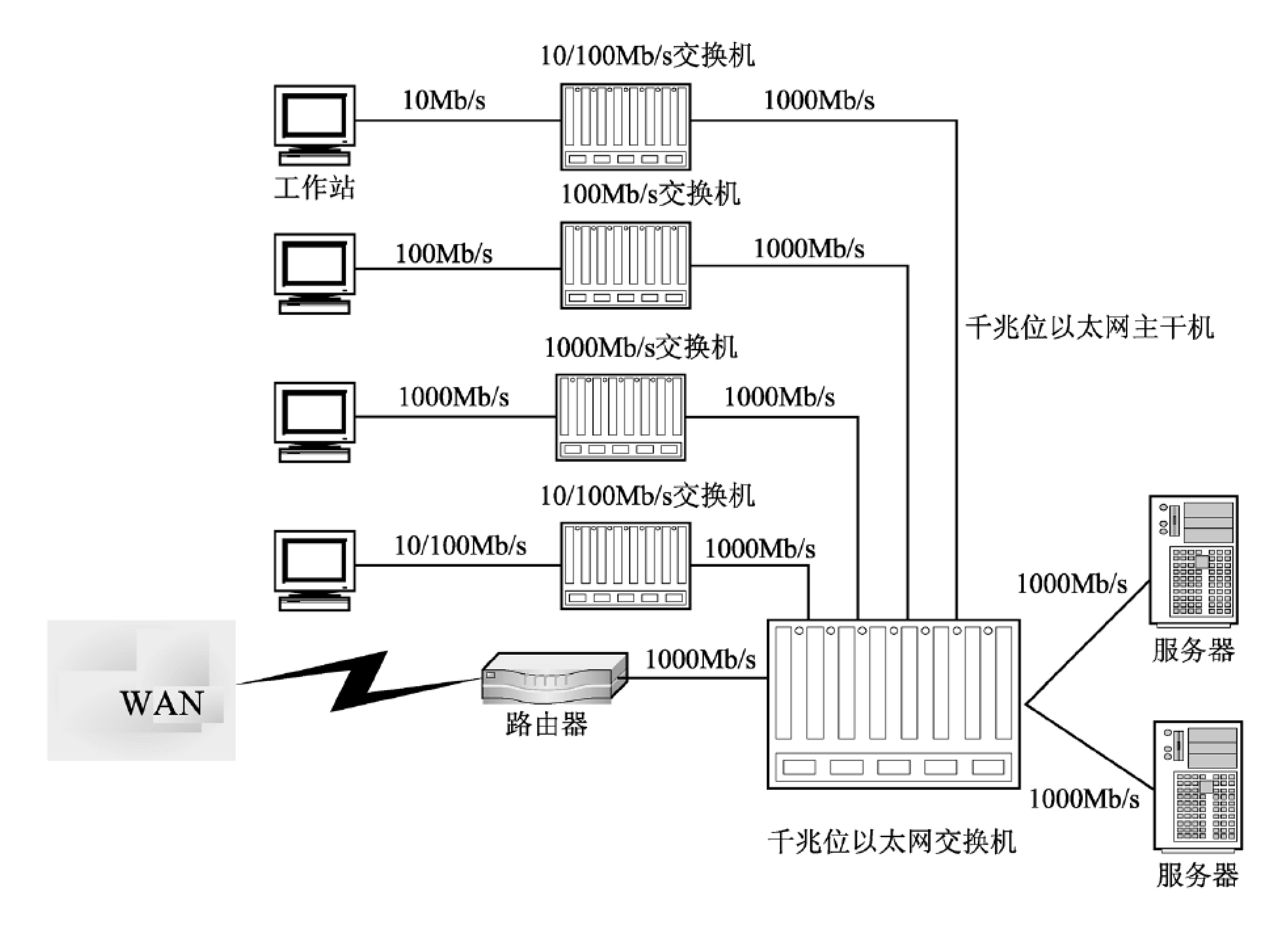


图 1-8　千兆位以太网与多个交换机的连接示意

1.2.1.6　万兆以太网

1. 10Gb/s 以太网

2002 年，IEEE 802.3ae 10Gb/s 以太网标准发布，以太网的发展势头又得到了一次增强。

物理层：IEEE 802.3ae 大体分为两种类型，一种是与传统以太网连接，速率为 10Gb/s 的 LAN PHY；另一种是 SDH/SONET 连接，速率为 9.58464Gb/s 的 WAN PHY。

传输介质层：IEEE 802.3ae 目前支持 9μm 单模光纤、50μm 多模光纤和 62.5μm 多模光纤。

数据链路层：IEEE 802.3ae 目前继承了 IEEE 802.3 以太网的帧格式和最大/最小帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，不影响上层应用，进而降低了升级风险。与传统的以太网不同，IEEE 802.3 仅支持全双工方式，而不支持单工和半双工方式，不采用 CSMA/CD 机制。IEEE 802.3ae 不支持自协商，可简化故障定位，并提供广域网物理层接口。

2. 40Gb/s 以太网

未来两年内，以太网最高数据传输速率将可望提高至 40Gb/s。Cafiero 称，业内将 40Gb/s 而非 100Gb/s 确定为以太网下一步发展目标的重要原因在于，与 100Gb/s 以太网相比，研发 40Gb/s 以太网在技术上面临的挑战相对较小，更为切实可行。与此同时，Cafiero 还指出，实际上，借助新发布的 Supervisor Engine 720 引擎，Cisco 公司的 Catalyst 6500 旗舰级企业交换平台目前已可以为每一接口卡提供 40Gb/s 的数据传输速率支持。Cafiero 还指出，新型以太网技术成功的关键在于能够推动单位数据传输成本的下降。

1.2.1.7　局域网交换技术

1. 共享型以太网

所谓共享型以太网，即在一个逻辑网络上的每一个工作站都处于一个相同的网段上。以太网采用 CSMA/CD 机制，整个系统处在一个碰撞域范围中，系统中每个站点都可能往媒体上发送帧，那么每个站点要占用媒体的几率就是(10Mb/s)/*n*，其中 *n* 为站点数。这种冲突检测方法保证了只能有一个站点在总线上传输。如果有两个站点试图同时访问总线并传输数据，就意味着“冲突”发生了，两站点都将被告知出错。然后它们都被拒发，并将等待一段时间以备重发。

这种机制就如同许多汽车抢过一座窄桥，当两辆车同时试图上桥时，就发生了“冲突”，两辆车都必须退出，然后再重新开始抢行。当汽车较多时，这种无序的争抢会极大地降低效率，造成交通拥堵。

网络也是一样，当网络上的用户量较少时，网络上的交通流量会较小，冲突也就较少发生，在这种情况下冲突检测法效果较好；当网络上的交通流量增大时，冲突也增多，同进网络的吞吐量也将显著下降；在交通流量很大时，工作站可能会被一而再、再而三地拒发。

2. 交换型以太网

为了解决共享以太网的问题，产生了交换型以太网。用交换机代替 Hub，在交换机上同时存在多个端口间的通道，就是说系统同时存在多个碰撞域，每一个碰撞域的一对端口都独占带宽(一个享有发送带宽，另一个享有接收带宽)，整个系统的带宽与交换机所具有的端口数有关。可以认为，若每个端口为 10Mb/s，则整个系统带宽可达 10Mb/s×*n*，其中 *n* 为端口数；若 *n*=10，则系统带宽可达 100Mb/s。

3. 全双工以太网

传统的共享型以太网只以半双工模式工作，即网络在同一时间要么发送数据，要么接收数据，而不能同时发送数据和接收数据。全双工以太网与传统半双工以太网技术之间的区别在于：每个端口和交换机背板之间都存在两条逻辑通道。这样，每一个端口就可以同时接收和发送帧，不再受 CSMA/CD 的约束，在端口发送帧时不再发生帧的碰撞，已无碰撞域的存在。这样一来，端口之间媒体的长度仅受到数字信号在媒体上传输衰变的影响，而不像传统以太网半双工传输时还要受到碰撞域的约束。其优点是，传输速度加快，对于光纤传输介质，传输距离变长。

1.2.1.8　局域网设备

计算机网络的组成可分为硬件与软件两大部分：硬件部分包括文件服务器、工作站、网卡、传输媒介、接头、网络中的设备、不间断电源系统(UPS)、打印机等；软件部分则包括网络操作系统(如 Windows NT、Linux、Novell、Netware 等)、网络管理系统和应用软件系统。

1. 服务器与工作站

服务器的主要功能是通过网络操作系统控制和协调网络各工作站的运行，处理和响应

各工作站同时发送来的各种网络操作要求，提供网络服务。工作站是网络各用户的工作场所，通常是一台微机或终端。

根据应用类型，网络服务器可分为文件服务器、应用程序服务器、通信服务器等几大类。通常，一个网络至少有一个文件服务器，网络操作系统及其实用程序和共享硬件资源都安装在文件服务器上。

按照网络服务器的设计思想分类，一般把服务器分为 3 种类型：一种是入门级服务器，有时也称为 PC 服务器；另一种是工作组级服务器，在中小企业的业务部门中使用，有时也称为部门级或工作组级服务器；还有一种是企业级服务器，一般担当企业的整体网络部署。

2. 网卡

网卡(Network Interface Card，NIC)也称为网络适配器，是连接计算机与网络的硬件设备。网卡插在计算机或服务器的扩展槽中，通过网线(如双绞线、同轴电缆或光纤)与网络交换数据、共享资源。在网络中，网卡的任务是双重的：一方面它负责接收网络上传过来的数据包，解包后将数据通过主板上的总线传输给本地计算机；另一方面它将本地计算机上的数据打包后送入网络。

3. 传输介质

1) 同轴电缆

同轴电缆抗干扰性好、频带较宽、数据传输稳定、价格适中、性价比高。同轴电缆中央是一根内导体铜质芯线，外面依次包有绝缘层、网状编织的外导体屏蔽层和塑料保护层。

通常按特性阻抗数值的不同，可将同轴电缆分为 50Ω 基带同轴电缆和 75Ω 宽带同轴电缆。前者用于传输基带数字信号，是早期局域网的主要传输媒体；后者是有线电视系统(CATV)中的标准传输电缆，在这种电缆上传输的信号采用了频分复用的宽带模拟信号。

50Ω 基带同轴电缆可分为粗缆和细缆两类。粗缆用于 10Base5 以太网，最大干线段长度为 500m，最大网络干线电缆长度为 2.5km，每条干线段支持的最大节点数为 100 个，收发器之间的最小距离为 1.5m，收发器电缆的最大长度为 50m；细缆用于 10Base2 以太网，最大干线段长度为 185m，最大网络干线电缆长度为 925m，每条干线段支持的最大节点数为 30 个，BNC-T 型连接器之间的最小距离为 0.5m。使用基带同轴电缆组网，需要在两端连接 50Ω 的反射电阻，又称终端匹配器。

2) 双绞线

双绞线是由两条导线按一定扭矩相互绞合在一起的类似于电话线的传输媒体，每根线加绝缘层并用颜色来标记。成对线的扭绞旨在使电磁辐射和外部电磁干扰减到最小。使用双绞线组网时，双绞线与网卡、集线器的接口称 RJ-45，俗称水晶头。

双绞线分为屏蔽双绞线和非屏蔽双绞线，STP 双绞线内部包了一层皱纹状的屏蔽金属物质，并且多了一条接地用的金属铜丝线，因此它的抗干扰性比 UTP 双绞线强，阻抗值通常为 150Ω。对于 UTP 双绞线，其阻抗值通常为 100Ω，每条双绞线最大传输距离为 100m。

双绞线的制作有两种方法：一种是直通线，即双绞线的两个接头都按 568B 线序标准连接；另一种是交叉线，即双绞线的一个接头按 EIA/TIA 568A 线序连接，另一接头按 EIA/TIA 568B 线序连接。

3)　光纤

光纤是新一代的传输介质，与铜质介质相比，它具有一些明显的优势。因为光纤不会向外界辐射电子信号，所以使用光纤介质的网络无论是在安全性、可靠性还是在传输速率等网络性能方面都有了很大的提高。

根据光在光纤中的传输方式，可将光纤分为两种类型：多模光纤和单模光纤。

4)　无线传输

无线传输主要分为无线电、微波、红外线及可见光几个波段。

无线电微波通信在数据通信中占有重要地位。微波的频率范围为 300MHz～300GHz，但主要使用 2～40GHz 的频率范围。微波通信主要有两种方式，即地面微波接力通信和卫星通信。

4.　网络互连设备

常用的网络互连设备有中继器、集线器、网桥、交换机、路由器以及网关等。

1)　中继器

中继器(Repeater)是网络物理层的一种介质连接设备，它工作在 ISO/OSI 参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时，可用中继器将该局域网的范围进行延伸。

2)　集线器

集线器(Hub)从工作原理上看就是一个多端口中继器，起到一个信号分散器的作用，它也工作在 ISO/OSI 参考模型的第一层(物理层)，通过一个端口接收信号，然后再发送到其他所有端口。它是在局域网上被广泛使用的网络设备，可以用来将若干台计算机通过双绞线或同轴电缆连到集线器，从而构建一个局域网。

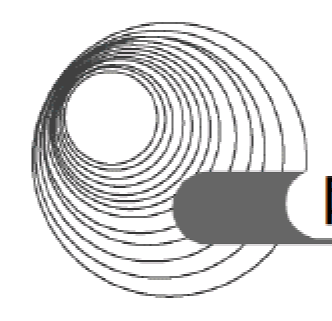
3)　网桥

网桥(Bridge)工作在 ISO/OSI 参考模型的第二层(数据链路层)，与高层协议无关，因此只能连接具有相同高层协议的网络。网桥的工作原理是，通过数据链路层的逻辑链路控制子层选择子网路径，接收完整的 MAC 数据帧并进行差错校验，再根据 MAC 中的源或目的地址决定帧的去向。如果是传给本网段的某一站点，则不予转发；如果目的地址是其他网络段的，则将它连接的所有网络段转发该 MAC 帧。在转发该帧之前，网桥对帧的内容和格式不做修改或仅作少量的修改后发送到物理层，再由物理层的传输介质发送到另外一个子网。

数据链路层连接两个局域网络段指的是网间通信从网桥传送，网内通信被网桥隔离。当网络负载重而导致性能下降时，用网桥可将其分为两个或多个网络段，从而最大限度地缓解网络通信繁忙的程度，提高通信效率。

4)　交换机

集线器虽然有多个端口，但同一时间只允许一个端口发送或接收数据；而交换机(Switch)则是采用程控交换机的原理设计的，允许多对端口同时发送或接收数据，每一个端口独占整个带宽，从而提供了一种提高数据传输速率的方法。交换机能够将以太网的速率提高至真正的 10Mb/s 或 100Mb/s。交换机工作在 ISO/OSI 参考模型的第二层(数据链路层)。目前局域网内广泛采用交换机设备。



5) 路由器

当两个不同类型的网络彼此相连时，必须使用路由器(Router)。路由器工作在 ISO/OSI 参考模型的第三层(网络层)，能够提供路由选择、流量控制、协议转换、分组过滤、子网分割等功能。可广泛应用于局域网之间、局域网与广域网之间以及广域网之间的互联。路由器的互联能力强，可以执行复杂的路由选择算法，处理的信息量比网桥多，但处理速度比网桥慢。

路由器在局域网系统中的应用如下。

- 局域网互联：连接多个局域网系统并实现局域网系统之间的数据转发。
- 局域网隔离：连接多个局域网系统并实现局域网系统之间的数据隔离。
- 局域网与广域网互联：局域网通过路由器连接广域网，实现对远程主机的访问。

6) 网关

当连接两个结构完全不同的网络时，必须使用网关(Gateway)。网关又称为协议变换器，它工作于传输层及其以上的层次，是用于在不同网络之间实现协议转换的专用网络通信设备。

网关可以设在服务器、微型机或大型机上。常见的网关有以下 4 种。

(1) 电子邮件网关：可以从一种类型的系统向另一种类型的系统传输数据。

(2) IBM 主机网关：可以在一台个人计算机与 IBM 大型机之间建立和管理通信。

(3) 互联网网关：允许并管理局域网和互联网间的接入，可以限制某些局域网用户访问互联网。

(4) 局域网网关：可以使运行于 OSI 模型不同层上的局域网网段间相互通信。路由器甚至只用一台服务器就可以充当局域网网关。局域网网关也包括远程访问服务器。它允许远程用户通过拨号方式接入局域网。

1.2.1.9 计算机网络接入技术

终端远程接入局域网、局域网与局域网远程互联或局域网接入广域网，这些都必须借助于公共传输网络。

公共传输网络的接入技术主要有：公共交换电话网(PSTN)、综合业务数字网(ISDN)、X.25 分组交换网、数字数据网(DDN)、帧中继(FR)、异步传输模式(ATM)、数字用户线路(xDSL)、宽带网接入、HFC 和 Cable Modem 接入技术等。

1) PSTN 接入技术

所谓“拨号接入”，就是指通过普通电话线利用 Modem(Modulator Demodulator，调制解调器)使用 PSTN(Public Switched Telephone Network，公用交换式电话网)来传输数据，普通拨号 Modem 的最高速率为 56kb/s。其接入硬件需要具备一台调制解调器、一条电话线、集线器或交换机、代理服务器(网卡和 Modem 的连接端口)等。代理服务器可安装 WinGate、Sygate 等代理软件，以便代理局域网内的其他计算机访问 Internet。其拓扑图如图 1-9 所示。代理服务器的串行口 COM 通过串行线与 Modem 相连，网卡通过双绞线与交换机或集线器相连，并根据需求设置该网卡的 IP 地址(私有地址)，如 192.168.1.1，子网掩码为 255.255.255.0，局域网内其他计算机设置的 IP 地址与该服务器的网卡地址位于同一个网段内。

也可使用带有 PSTN 端口的路由器接入 Internet。其拓扑图如图 1-10 所示。

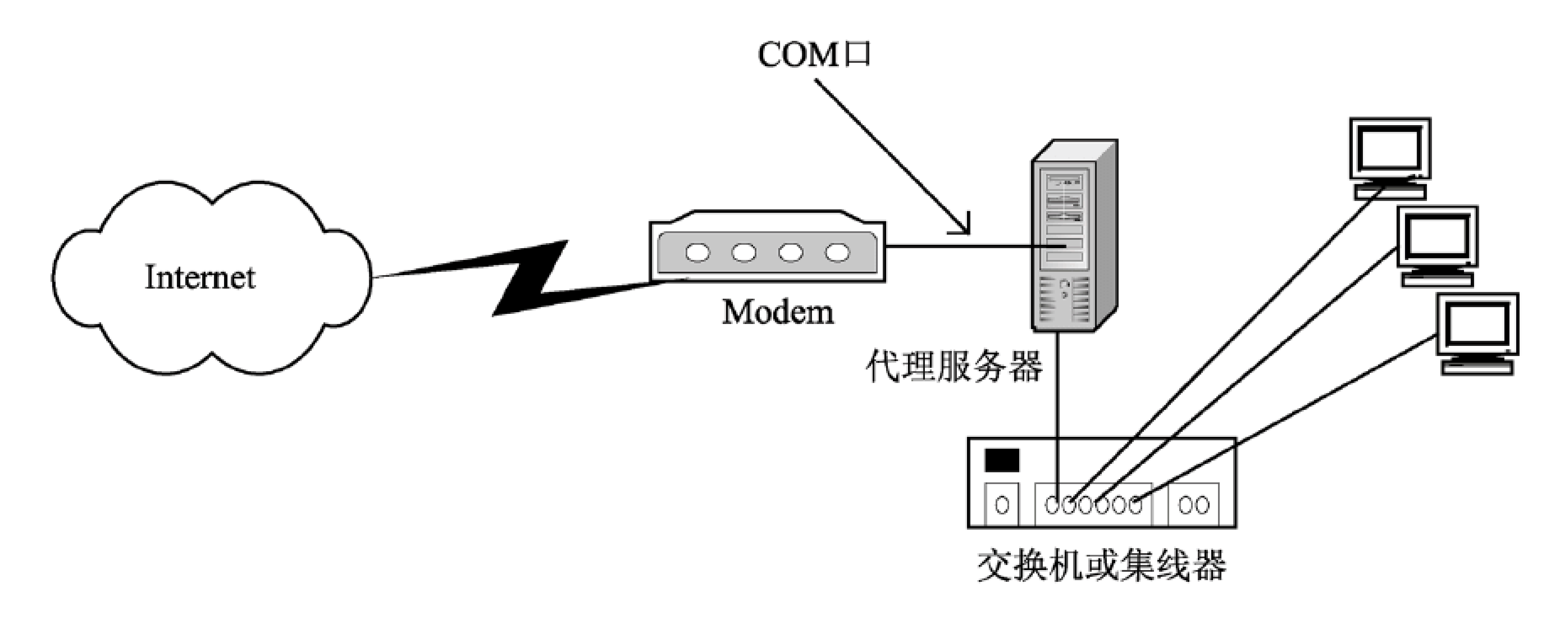


图 1-9　用调制解调器连接 Internet

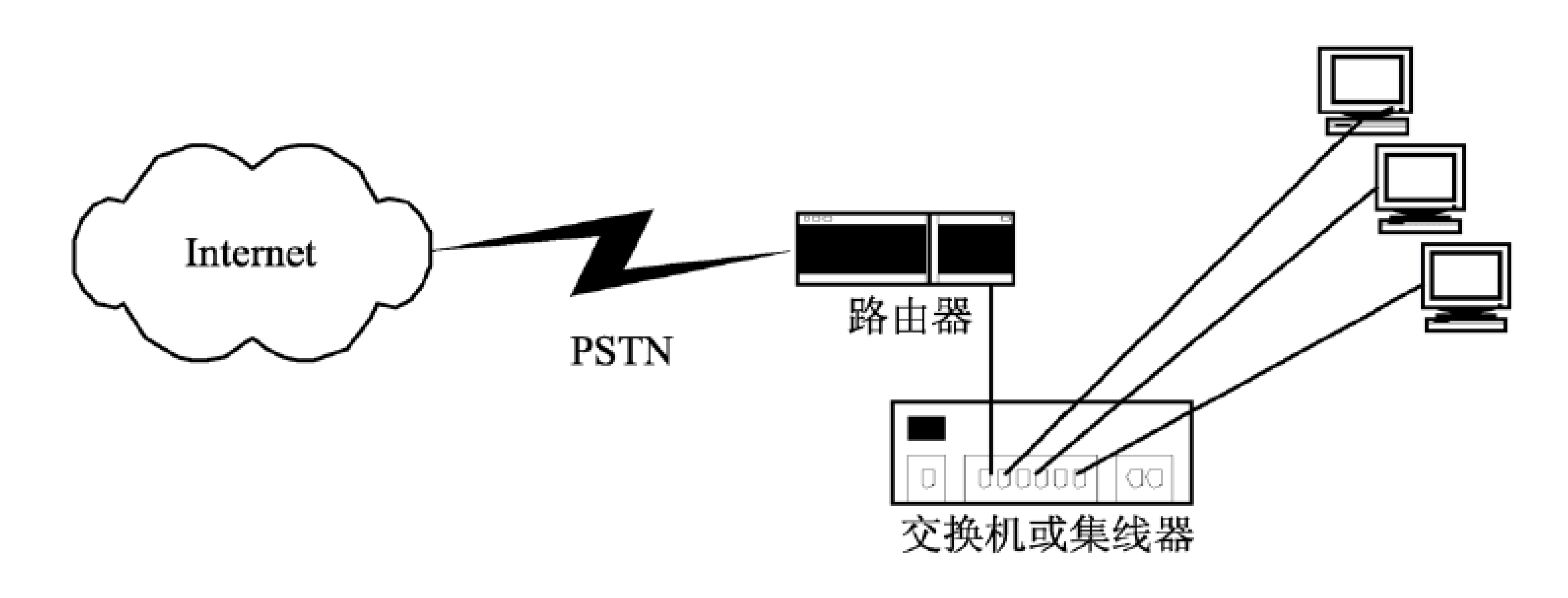


图 1-10　使用路由器接入 Internet

2)　ISDN 接入技术

ISDN 是 Integrated Services Digital Network(综合业务数字网)的缩写，能在一根普通电话线上提供语音、数据、图像等综合性业务。ISDN 在一对普通的电话用户线路上，提供两个双向的 64kb/s 的 B 通道和一个 16Kb/s 的 D 通道。B 通道是承载通道，可以传送语音和数据。两个 B 通道既可以单独使用，也可以捆绑起来传送数据，都可达到 128kb/s 的速率。ISDN 可连接 8 台终端或电话，有两台终端(如一部电话、一台计算机或一台数据终端)可以同时使用。对于用户而言，同样的一对普通电话线原来只能接一部电话机，而申请了 ISDN 后，通过一个称为 NT 的转换盒，就可以同时使用数个终端。在一根普通电话线上，可以提供以 64kb/s 速率为基础并可达到 128kb/s 上网速度的数字连接。

局域网用户可通过 ISDN 专线接入 Internet，其拓扑结构如图 1-11 所示。所需的硬件设备有 NT1、ISDN 专线、交换机或集线器、代理服务器(ISDN 卡和网卡)等。代理服务器可安装 WinGate、Sygate 等代理软件，以便代理局域网内的其他计算机访问 Internet。

局域网用户也可采用 ISDN 路由器接入 Internet，其拓扑图如图 1-12 所示。

3)　ADSL 接入技术

ADSL 是英文 Asymmetrical Digital Subscriber Loop(非对称数字用户环路)的缩写，ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术，它利用现有的一对电话铜线，为用户提供上、下行非对称的传输速率(带宽)。非对称主要体现在上行速率(最高 640kb/s)和下行速率(最高 8Mb/s)的非对称性上。上行(从用户到网络)为低速的传输，可达 640kb/s；下行(从网络到用户)为高速传输，可达 8Mb/s。在不影响原有语音信号的基础上，扩展了已有电话线路的功能。

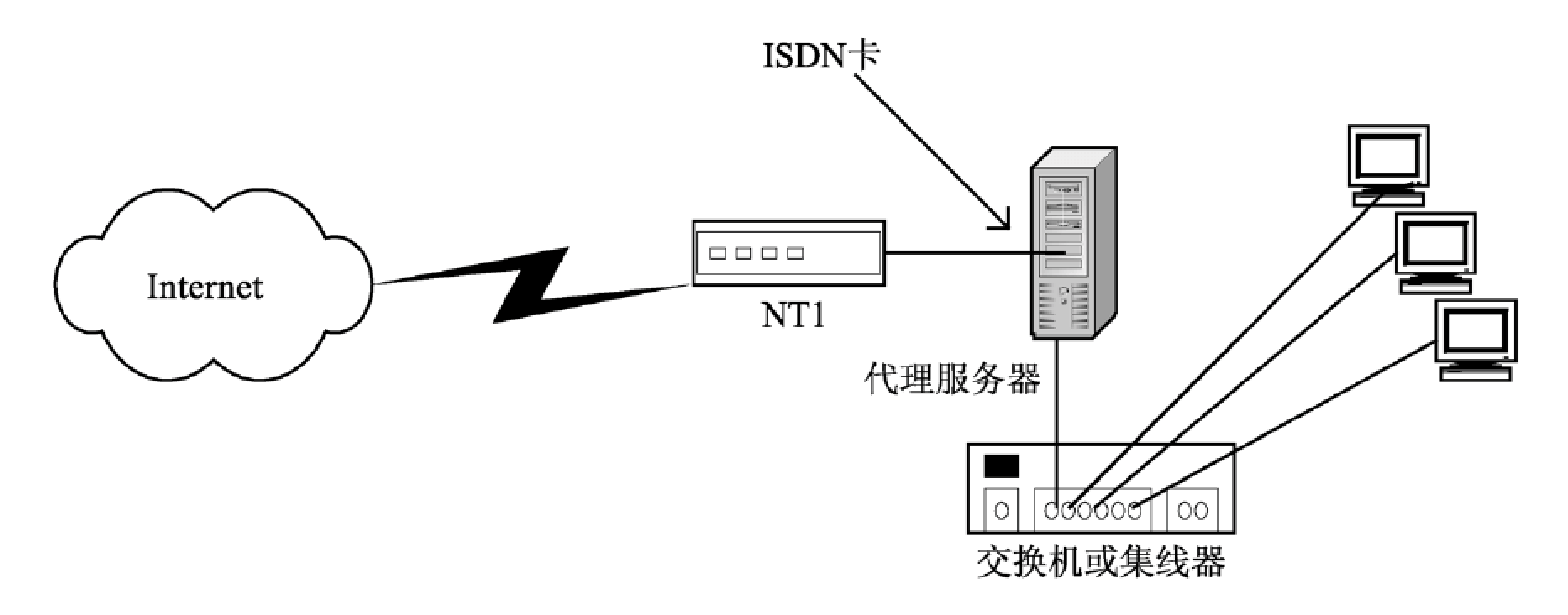


图 1-11　局域网使用 ISDN 专线接入 Internet

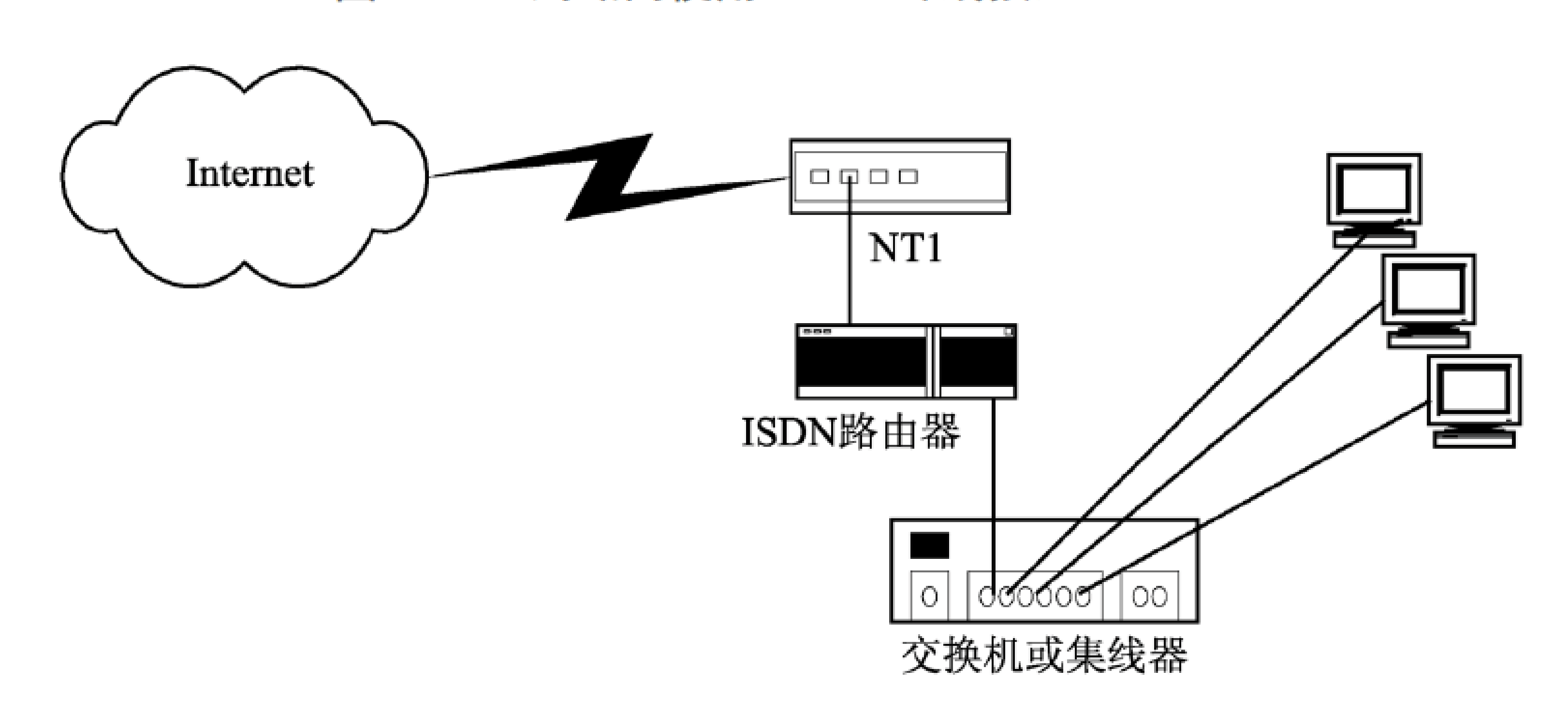


图 1-12　局域网使用 ISDN 路由器接入 Internet

局域网用户可通过 ADSL 接入 Internet，其拓扑图如图 1-13 所示。所需的硬件设备有语音/数据分离器、ADSL 专线、交换机或集线器、代理服务器(两块网卡)等。代理服务器上连接 ADSL Modem 的那一块网卡设置电信公司提供的 IP 地址、子网掩码、DNS、网关等参数，内网可设置私有地址，并安装代理服务软件，以便代理局域网内的其他计算机访问 Internet。

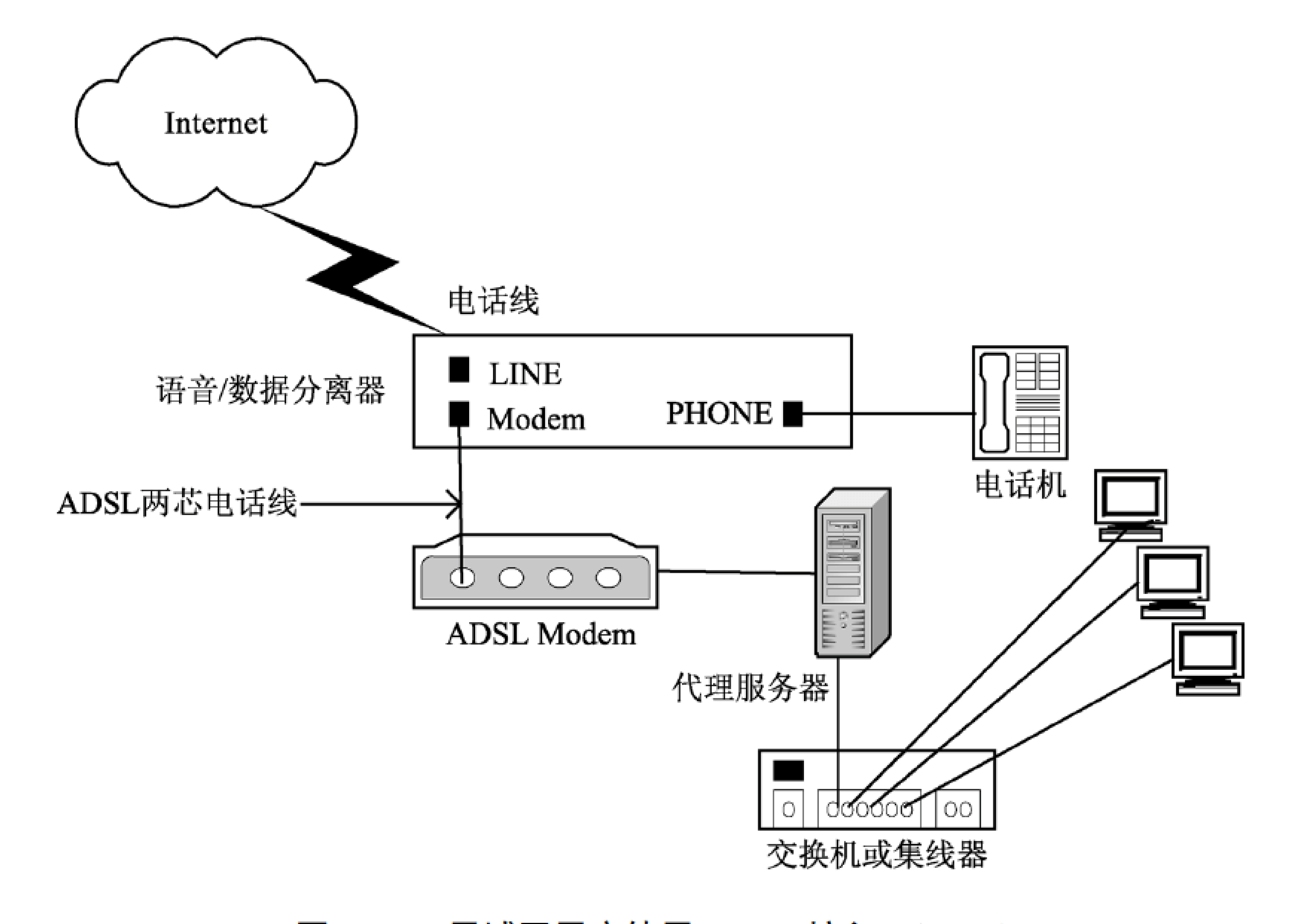


图 1-13　局域网用户使用 ADSL 接入 Internet

局域网用户也可利用 ADSL 路由器接入 Internet，其拓扑图如图 1-14 所示。

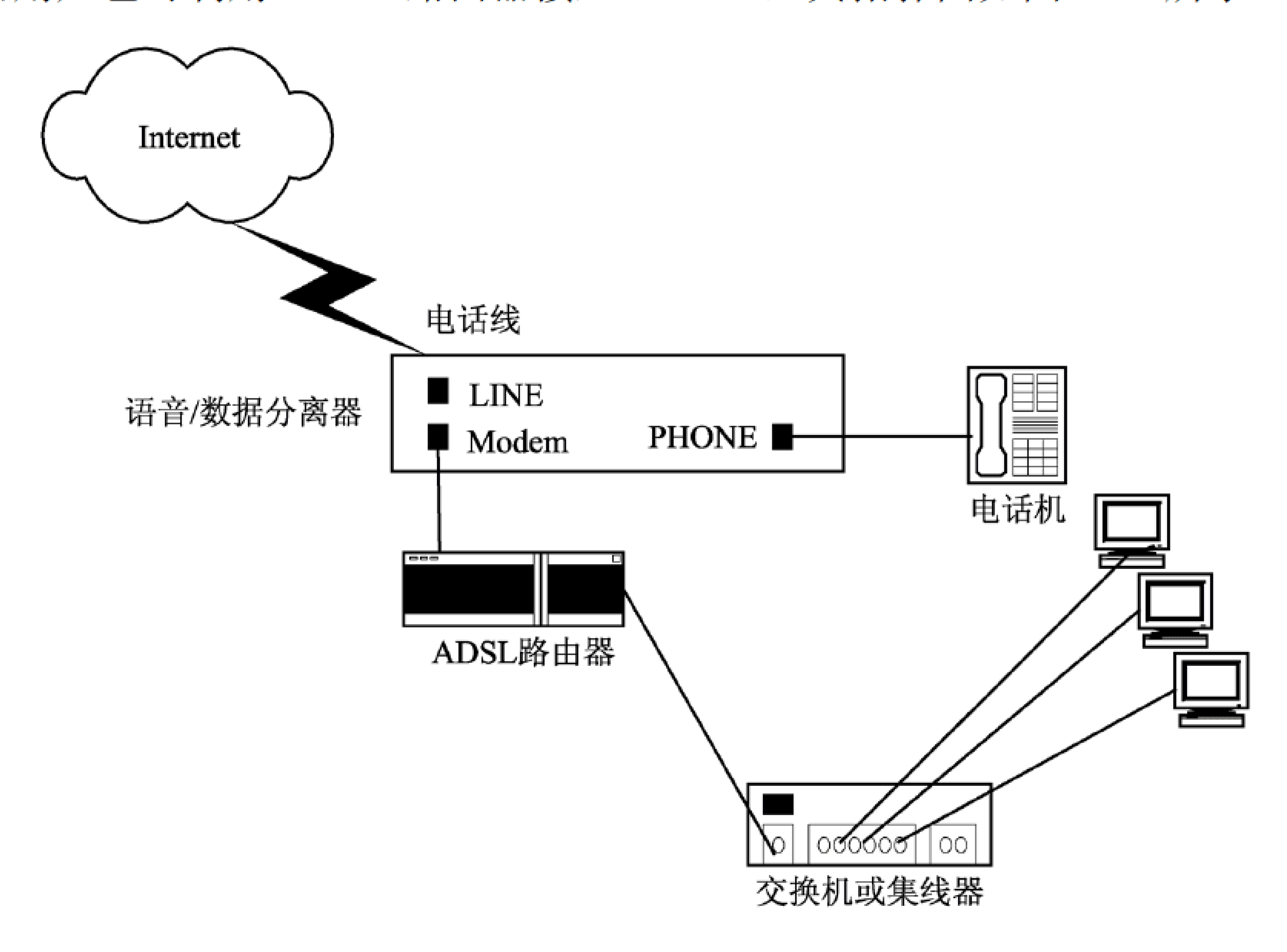


图 1-14　局域网使用 ADSL 路由器接入 Internet

4)　宽带网接入技术

宽带网，也称为“IP 城域网”。它是在城市范围内以多种传输媒介为基础，采用 TCP/IP 协议，通过路由器组网，实现 IP 数据包的路由和交换传输。

IP 城域网的接入方式目前一般分为 LAN 接入(用网线)和 FTTX 接入(用光纤)。LAN 接入是指从城域网的节点经过交换机和集线器将网线接入到用户家中。FTTX 接入是指光纤直接接入到用户家中，即光纤到户(FTTH)或光纤到桌面(FTTD)，它是未来宽带网络发展的方向。

宽带 IP 网以光纤通信为基础，以成熟的 IP 技术为核心，采用路由器和交换机等设备组网，可为用户提供 10Mb/s、100Mb/s、1000Mb/s 可选接入速率。其速率是目前电话拨号上网的 170 多倍。

宽带 IP 网的建设目标是铺设光纤到小区，到大楼，最终以光纤到户为目标。目前一般采用光纤加局域网的方式实现群体用户接入宽带网络。其拓扑图如图 1-15 所示。

5)　HFC 和 Cable Modem 接入技术

HFC 网是光纤同轴电缆混合网，它是一种新型的宽带网络，采用光纤到服务区，而在进入用户的“最后 1 千米”采用同轴电缆，最常见的是有线电视网络。HFC 网络大部分采用传统的高速局域网技术，而 Cable Modem 是其中最重要的组成部分。

Cable Modem 可以译为电缆调制解调器或线缆调制解调器，它是一种将数据终端设备连接到有线电视网(CATV)，以使用户能够进行数据通信访问 Internet 等信息资源的设备。

6)　数据通信网接入技术

局域网用户还可以通过 DDN 网、X.25 网、帧中继网、ATM 网接入 Internet，其核心设备是路由器等网络终端接入设备。其拓扑结构如图 1-16 所示。

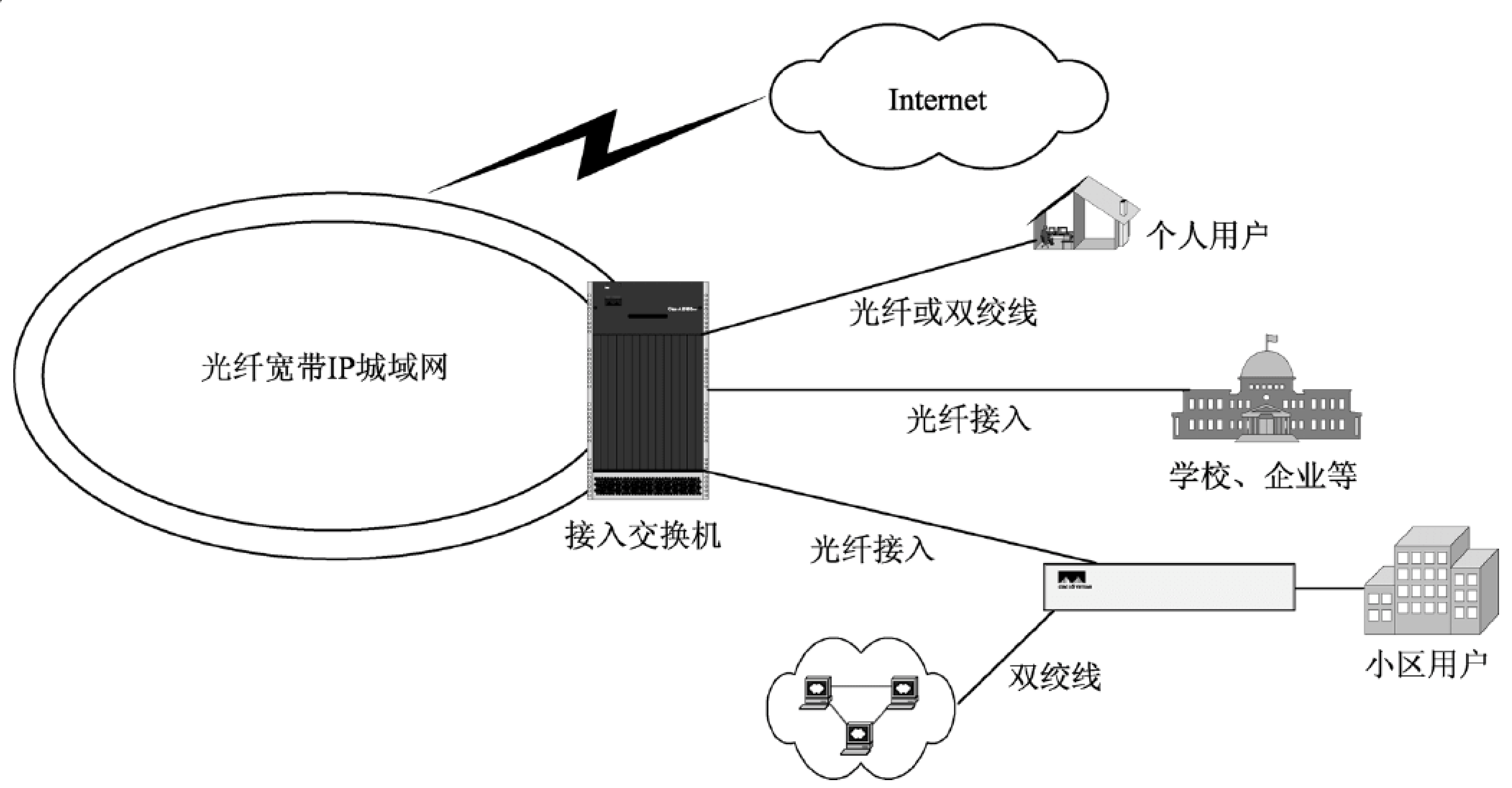


图 1-15　局域网宽带 IP 接入 Internet

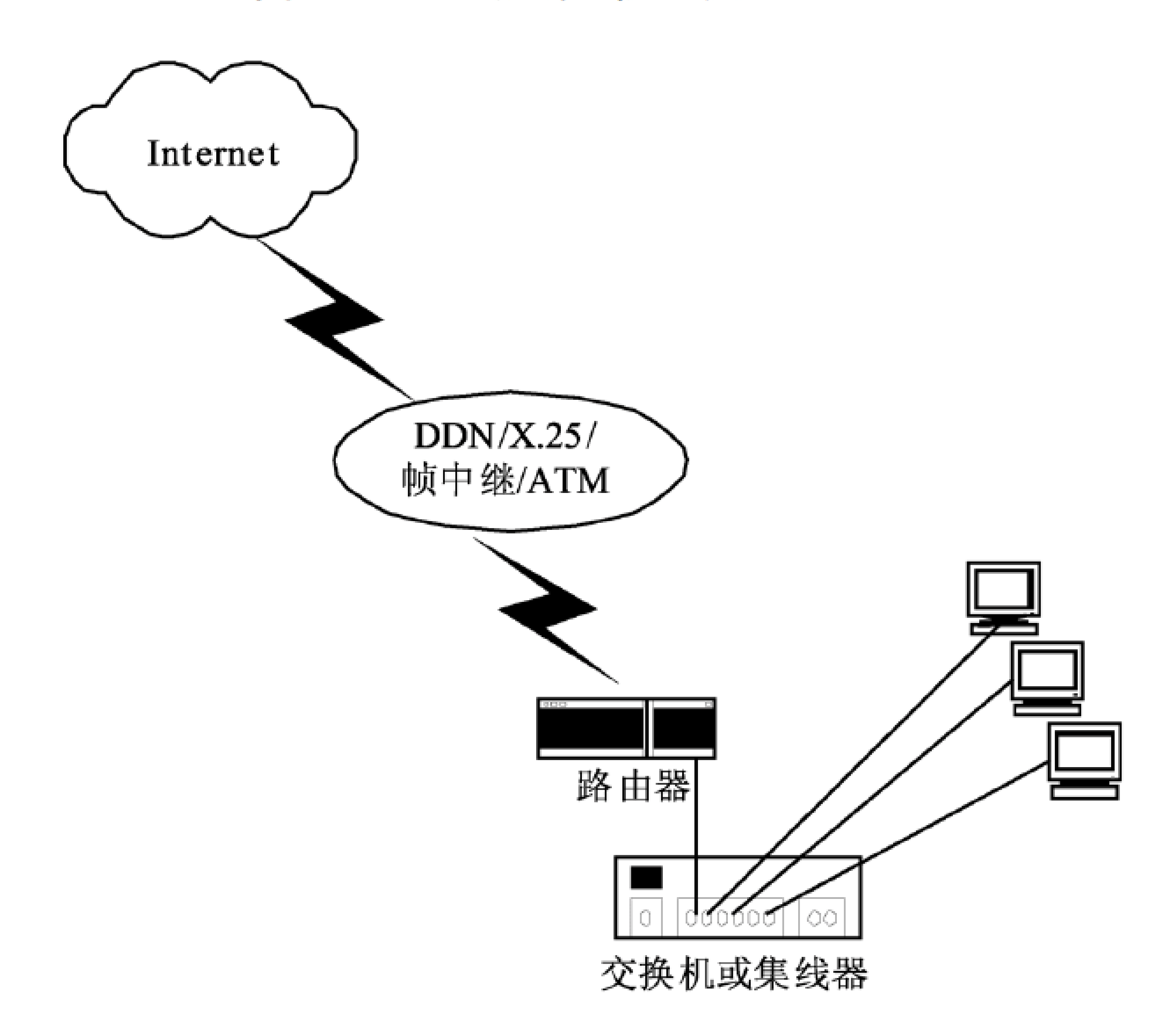


图 1-16　局域网使用数据通信网接入 Internet

(1)　X.25 分组交换网

X.25 是 CCITT 制定的在公用数据网上供分组型终端使用的，数据终端设备(DTE)与数据通信设备(DCE)之间的接口建议。它只是一个以虚电路服务为基础的对公用分组交换网接口的规格说明。它动态地对用户传输的信息流分配带宽，能够有效地解决突发性、大信息流的传输问题，分组交换网络同时可以对传输的信息进行加密有效的差错控制。

X.25 一般只用于要求传输费用少，而远程传输速率要求又不高的广域网环境。其速率为 9600b/s～64kb/s。

(2)　数字数据网

数字数据网(DDN)是利用数字通道提供半永久性连接电路，向用户提供端到端的中高速率、高质量的数字专用电路，全程实现数字信号透明传输的数据传输网。DDN 网通常由 4

部分组成，包括本地传输系统、复用与交叉连接系统、局间传输与同步系统和网络管理系统等。DDN 干线主要采用光缆、数字微波与卫星信道，所提供的信道是非交换型的半永久电路，通常由电信部门在用户申请时设定，修改并非经常性的。

DDN 采用脉冲编码调制(PCM)的数字中继方式，传输距离远，具有传输速度快、质量好、性能稳定和带宽利用率高等优点。其速率可达 2Mb/s。

(3) 帧中继

帧中继是为了克服 X.25 的缺点，提高性能而发展起来的一种高速分组交换与传输技术。它是一种减少节点处理时间的技术。帧中继认为帧的传送基本上不会出错，因此每个节点只要一知道帧的目的地址，就立即转发，大大减少了帧在每一个节点的时延，比传统的 X.25 的处理时间少一个数量级。

帧中继的设计目标主要是针对局域网之间的互联，它以面向连接的方式，合理的数据传输率和低廉的价格提供数据通信服务。帧中继的主要思想是“虚拟租用线路”。帧中继采用帧作为数据传送单元，网络的带宽根据用户帧传输的需要，可以采用统计复用的方式动态分配，可以充分复用网络资源，从而提高了中继带宽的利用率，尤其对突发信息的适应性比较强。帧中继用户的接入速率为 64kb/s～2Mb/s。

(4) 异步传输模式(ATM)

ATM 是 Asynchronous Time division multiplexing 的缩写，译为“异步传输模式”，它是以高速分组传送模式为主，综合电路传输模式优点的一种宽带传输模式。

ATM 系统使用异步时分复用技术的快速分组交换方式，它将信息流分割成固定长度的 ATM 信元，能比较容易地实现各种信息流混合在一起的多媒体通信，能根据业务类型、传输速率等要求动态分配有效容量，对高速信息元传输频次高，对低速信息元传输频次低。因此 ATM 能采用单一的交换方式，支持从窄带语音、数据传输到高清晰度电视(High Definition Television，HDTV)等范围极广的各种业务。

ATM 信元是固定长度的分组，并使用空闲信元来填充信道，从而使信道被分为等长的时间小段。每个信元共有 53 个字节，分为两个部分。前面 5 个字节为信头，主要完成寻址的功能；后面的 48 个字节为信息段，用来装载来自不同用户、不同业务的信息。ATM 接入的速率可达 155～622Mb/s。

1.2.2 典型例题分析

例 1 目前局域网广泛采用以太网技术。局域网互联时，通常采用中继器、集线器、网桥、交换机、路由器、网关等设备，请简要回答下列问题。

【问题 1】以太网的标准是什么？

【问题 2】中继器、集线器、网桥、交换机、路由器、网关分别工作在 ISO/OSI 参考模型的哪一层？

【问题 3】简述路由器的特点。

分析：问题 1 是考查以太网的概念，要求考生对以太网的标准有所了解，属于识记层次，较容易。

问题 2 是考查局域网互联设备工作在 ISO/OSI 参考模型的哪一层。中继器是网络物理层的一种介质连接设备，它工作在 ISO/OSI 参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时，可用中继器将该局域网的范围进行延伸。集线器从工作原理上看就是一个多端口中继器，它起到一个信号分散器的作用，它也工作在 ISO/OSI 参考模型的第一层(物理层)，它通过一个端口接收信号然后再发送到其他所有端口。网桥工作在 ISO/OSI 参考模型的第二层(数据链路层)，负责接收和转发数据帧，并对数据帧进行管理。交换机从工作原理上看就是一个多端口网桥，它利用存储转发和过滤技术来分割网段，使局域网整体带宽得到成倍提高。路由器工作在 ISO/OSI 参考模型的第三层(网络层)，它能够在复杂网络中为网络数据的传输自动进行路径选择。网关工作在 ISO/OSI 参考模型的传输层及其以上的层次，用于在不同网络之间实现协议转换的专用网络通信设备。

问题 3 考查路由器的特点。

答案：

【问题 1】以太网的标准是 IEEE 802.3。

【问题 2】中继器工作在 ISO/OSI 参考模型的第一层、集线器工作在 ISO/OSI 参考模型的第一层、网桥工作在 ISO/OSI 参考模型的第二层、交换机工作在 ISO/OSI 参考模型的第二层、路由器工作在 ISO/OSI 参考模型的第三层、网关工作在 ISO/OSI 参考模型的传输层及其以上的层次。

【问题 3】路由器的特点如下。

(1) 更强的异种网络互联能力。路由器不仅能实现不同类型的局域网互联，而且可以用于局域网与广域网、广域网与广域网的互联，同时，它还提供不同网络地址格式的转换功能。

(2) 有较好的拥挤控制能力。路由器具有各种解决拥挤的方法，而网桥只能通过加大缓存来局部解决拥挤问题。同时，路由器可以隔离广播信息，避免出现广播风暴。

(3) 具有防火墙功能。路由器通常有多种隔离信息包的方法，从而进一步加强网络的安全保密性，防止网络系统和系统内的数据遭到攻击和破坏。

(4) 便于网络管理和维护。路由器连接的各个网络仍是独立的子网，便于各自管理和维护。并且，通过路由器提供的网管功能，可以随时对各子网的工作状况进行监视和控制，及时发现和解决可能出现的问题。

例 2 阅读以下说明，回答问题。

【说明】

图 1-17 是某办公局域网的结构图，采用 8 口 Hub 将客户机、打印机及服务器相连，形成一个小型的办公网络。

【问题 1】该网络采用的媒体访问控制技术是什么？

【问题 2】局域网的主要网络拓扑有哪些？图 1-17 采用了哪种网络拓扑？

【问题 3】Hub 与服务器、客户机之间采用什么传输介质？

分析：问题 1 考查共享型以太网的概念。用 Hub 组建的以太网为共享型以太网，采用 CSMA/CD 媒体访问控制技术是它的特征。

问题 2 考查局域网的拓扑结构分类。局域网的拓扑结构通常分为三种，分别是总线型

拓扑结构、星型拓扑结构和环型拓扑结构。总线型结构使用同一媒体或电缆连接所有端用户，也就是说，连接端用户的物理媒体由所有设备共享。星型结构存在着中心节点，每个节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中心节点来转接。环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户到另一个端用户，直到将所有端用户连成环型。

问题 3 考查局域网采用的传输媒体。在 Hub 组建的以太网中，局域网采用两端都装有同样的 RJ-45 型接头(水晶头)，每一个工作节点都需要一根双绞线电缆，用来连接工作节点上的网卡与集线器。

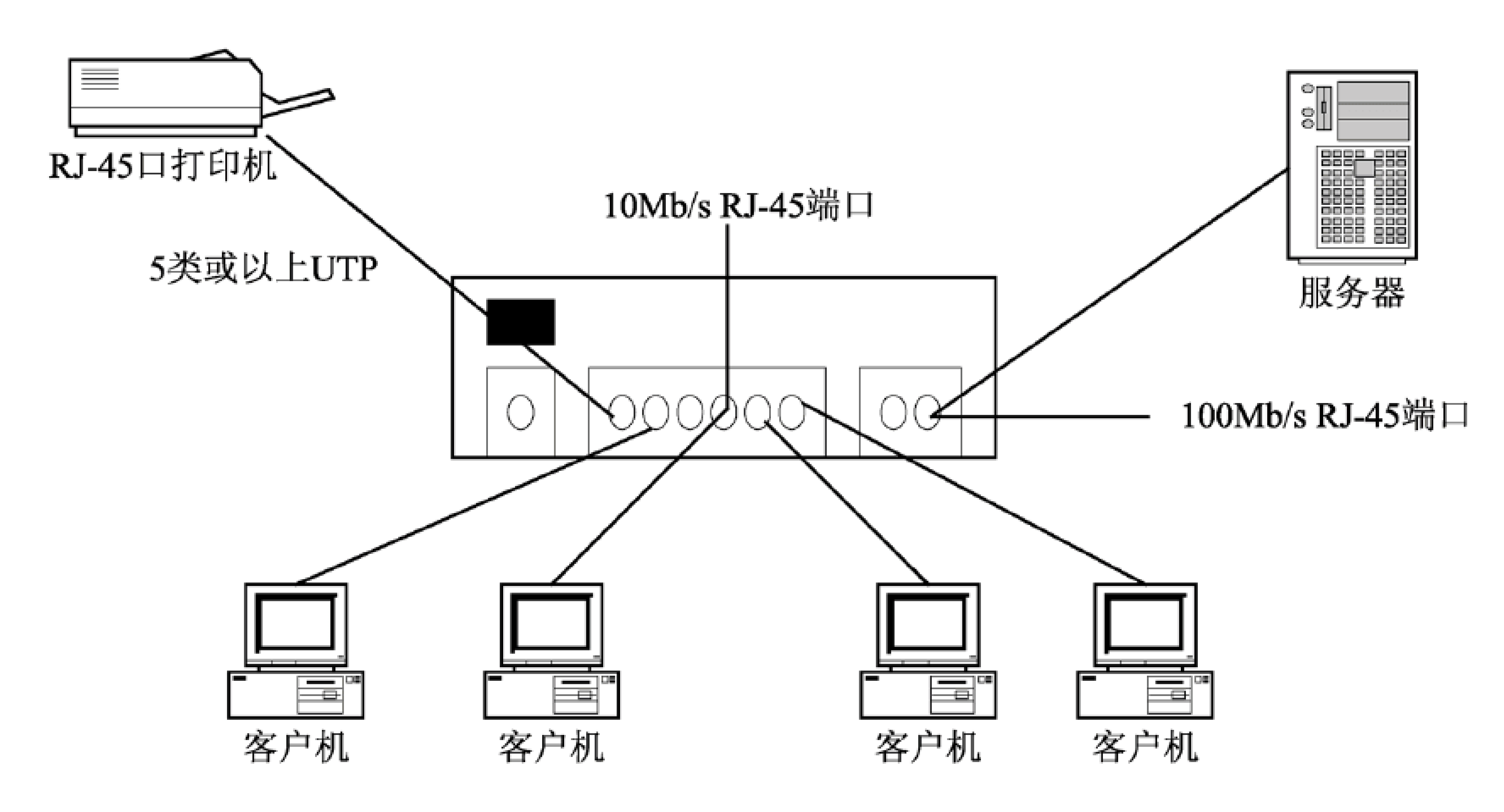


图 1-17　某办公局域网拓扑结构

答案：

【问题 1】CSMA/CD。

【问题 2】局域网在网络拓扑上主要采用了环型、星型和总线型结构。图 1-17 中采用的是星型拓扑结构。

【问题 3】双绞线。

例 3　简要回答有关局域网传输媒体的问题。

【问题 1】局域网的传输媒体包括哪些种类？

【问题 2】目前局域网上常用哪几种传输媒体？

【问题 3】目前局域网上能达到最高传输率的传输媒体是哪一种？

【问题 4】要获得最佳的数据传输安全保密性的传输媒体是哪一种？

分析：局域网的传输媒体主要有双绞线、同轴电缆、光缆和无线传输四大类。最常用的是双绞线和光缆，这与它们各自的特点是分不开的。一般短距离采用双绞线，长距离则使用光缆。

光纤利用全内反射来传输经信号编码的光束，能实现最高速率的传输。所以说目前局域网能达到最高传输率的传输媒体是光缆。

光纤不受电磁干扰或噪声的影响，这种特性允许其在很长的距离内进行高速数据传输，并能提供优良的安全保密性，所以说要想获得最佳的数据传输安全保密性，就要采用光缆

作为这种传输媒体。

答案：

【问题 1】传输媒体是收发双方之间进行通信的物理信号通路。用于局域网的传输媒体有双绞线、同轴电缆、光缆和无线传输媒体四类。

【问题 2】目前局域网常用的传输媒体为双绞线和光缆。

【问题 3】目前局域网上能达到最高传输率的传输媒体是光缆。

【问题 4】要获得最佳的数据传输安全保密性的传输媒体是光缆。

例 4　阅读以下说明，回答问题。

【说明】

某大型企业包括网络中心、管理部、生产部、市场部、财务部、人事部等部门，各部门内部都已经建设了自己的局域网系统。现要将企业内部各部门的局域网互联起来。建设企业内联网。

组网要求：能够实现企业内部各部门局域网系统的有效隔离，防止跨部门的非法访问；各部门之间根据需要可以有效互联通信，将信息由部门级共享提高企业级共享；各部门的计算机都可以连接访问 Internet。

【问题 1】请简述其实施方案并画出网络拓扑结构示意图。

【问题 2】简述路由器在局域网组网工程中的应用。

分析：根据用户需求可以总结出用户对现有局域网系统的三点要求：局域网隔离、局域网互联以及局域网与广域网互联。这恰好就是路由器在局域网系统中的三项应用。因此可以在组网方案中应用路由器作为网络互联设备。

答案：

【问题 1】各部门局域网之间通过路由器互联起来，通过配置路由器实现各部门之间的访问控制策略；路由器具有连接 Internet 的广域网端口，企业内部各部门局域网系统中的计算机可以通过路由器访问 Internet，其拓扑结构如图 1-18 所示。

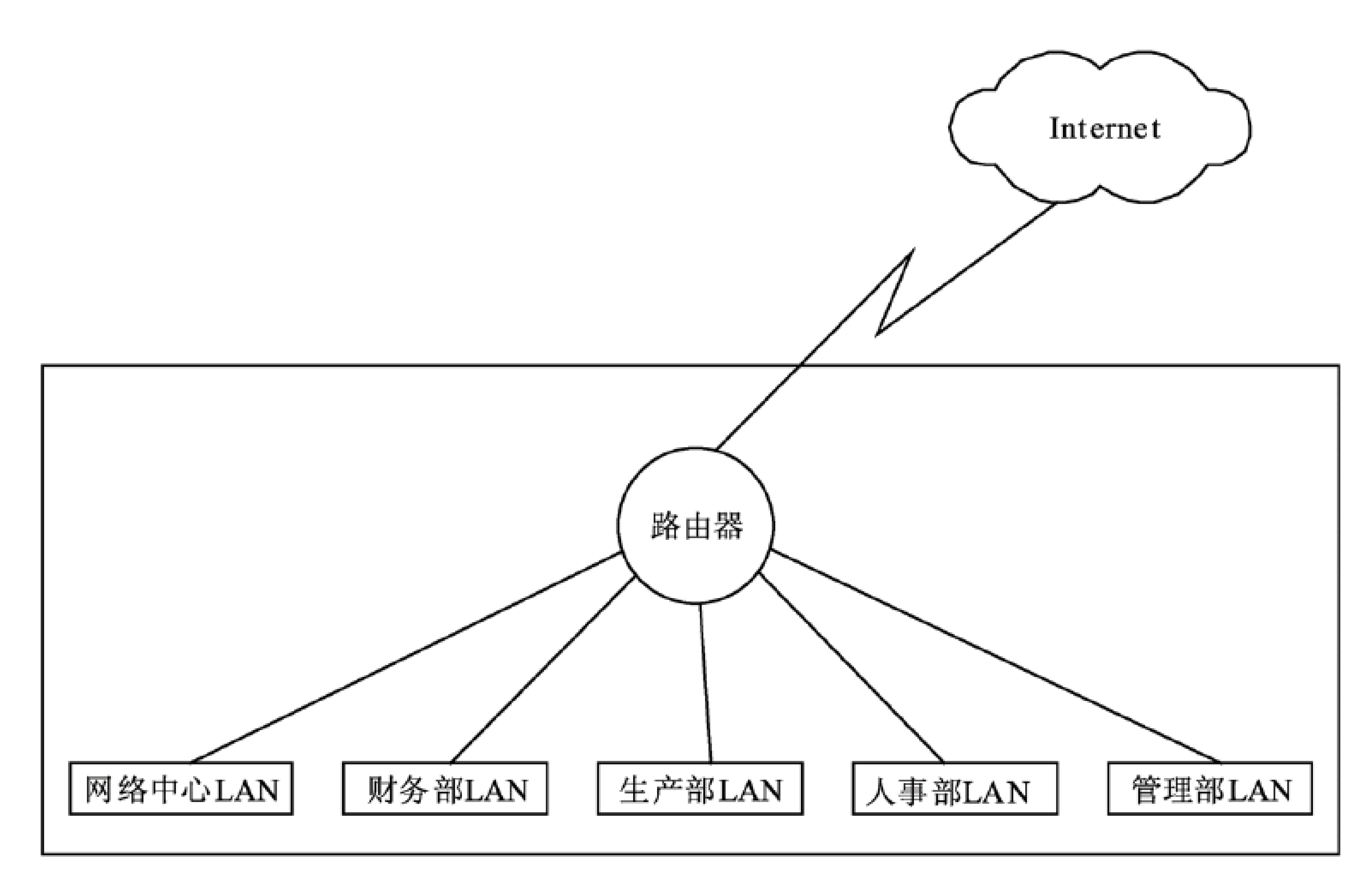


图 1-18　某企业内部网组网拓扑结构

【问题 2】路由器在局域网系统中的应用主要如下。

(1) 局域网互联：连接多个局域网系统并实现局域网系统之间的数据转发。互联的局域网系统可以是相同类型，也可以是不同类型。

(2) 局域网隔离：连接多个局域网系统并实现局域网系统之间的数据隔离。

(3) 局域网与广域网互联：局域网通过路由器连接广域网，实现对远程主机的访问。

1.2.3　同步练习

1．简要回答下列有关局域网的问题。

【问题 1】局域网需要 OSI 参考模型的哪几层？

【问题 2】局域网的标准主要是由哪个委员会制定的？

【问题 3】列出局域网常用的访问控制方式。

2．简要回答下列有关 10Mb/s 以太网的问题。

【问题 1】简述 10BaseT 以太网的组成。

【问题 2】简述 10BaseT 以太网系统的特点。

【问题 3】在 10BaseT 的收发器中，双绞线起什么作用？

【问题 4】试比较四种 10Base 以太网的物理性能。

3．按传输媒体类型划分快速以太网类型。

4．交换型以太网的中心设备是什么？与共享型以太网系统比较，交换型以太网系统有何特点？

5．10Mb/s 以太网、快速以太网以及千兆位以太网有何区别与联系？

6．对于工作在半双工模式的 24 口交换机，若每个端口的速率为 10Mb/s，则整个系统带宽可达多少？

7．简要回答下列问题。

【问题 1】哪些以太网产品支持全双工操作？

【问题 2】简述全双工以太网的技术特点(与传统半双工以太网相比)。

8．已知某局域网采用 CSMA/CD 媒体访问控制技术，其共享媒体最大跨距为 500m，物理层处理延迟时间为 10^{-5}s，传输媒体的数据传输率为 10Mb/s，试计算该网络的最小帧长度。

9．简要回答下列问题。

【问题 1】收发器的主要功能有哪些？

【问题 2】对于 10Mb/s 的以太网有哪几种收发器？

【问题 3】集线器在以太网系统中具有的主要功能。

1.2.4　同步练习参考答案

1．

【问题 1】局域网需要 OSI 中的物理层、数据链路层(数据链路层分为媒体访问控制子层和逻辑链路控制子层)。

【问题 2】IEEE 802 委员会。

【问题 3】局域网常用的访问控制方式有 3 种，分别是载波帧听访问/冲突检测(CSMA/CD)、令牌环访问控制法(Token Ring)和令牌总线访问控制法(Token Bus)。

2.

【问题 1】10BaseT 以太网的组成如下。

(1) 10BaseT 以太网系统由集线器、网卡和非屏蔽双绞线(3 类以上)组成。

(2) 网卡与集线器、集线器与集线器之间通过 RJ-45 连接器和双绞线实现互联和通信。

(3) 10BaseT 以太网系统中，单段媒体最大长度为 100m，可以通过 4 个集线器级联，连接 5 个媒体使最大跨距达 500m。

【问题 2】10BaseT 以太网系统的特点如下。

(1) 采用星型或树型拓扑结构，核心为集线器。

(2) 传输媒体采用 3 类、4 类或 5 类非屏蔽双绞线，发送与接收通道物理上分开，各占一根双绞线。

(3) 网络站点通过网卡上的 RJ-45 连接器和双绞线直接连接集线器。

【问题 3】双绞线的作用如下。

(1) 网卡上发送和接收分别使用一根双绞线，即一根双绞线发送信号，另一根作为信号接收使用。

(2) 当网卡与集线器相连接时，网卡上作为发送的那根双绞线正作为集线器接收使用；反之，网卡上作为接收的那根双绞线正作为集线器发送使用。

【问题 4】10Base 以太网的物理性能如下。

(1) 10Base5 使用外置收发器，传输媒体为价格较贵、需要专业化安装的直径 10mm、阻抗 50Ω 的粗同轴电缆，采用总线型拓扑结构，单段媒体最大长度为 500m，最多可使用 4 个中继器连接 5 段媒体使跨距最大达 2.5km，网卡通过 AUI 接口与媒体连接。

(2) 10Base2 在网卡上内置收发器，传输媒体使用价格便宜、安装简单的直径 5mm、阻抗 50Ω 的细同轴电缆，采用总线型拓扑结构，单段媒体最大长度为 185m，最多可使用 4 个中继器连接 5 段媒体使跨距最大达 925m，网卡通过 BNC 连接器和 T 型头与媒体连接。

(3) 10BaseT 在网卡上内置收发器，传输媒体使用便宜、安装简单的非屏蔽双绞线(3 类以上 UTP)，采用星型拓扑结构，单段媒体最大长度为 100m，可以通过 4 个集线器级联，连接 5 个媒体使最大跨距达 500m，网卡通过 RJ-45 连接器与媒体连接。

(4) 10BaseF 在网卡上内置收发器，传输媒体使用 62.5/125 多模光纤，采用星型拓扑结构，单段媒体最大长度为 2km，可以通过 1 个集线器级联，连接 2 个媒体段使最大跨距达 4km，网卡通过 ST 连接器与光纤连接。

3.

按传输媒体类型划分，快速以太网可分为 100BaseTX、100BaseFX、100BaseT4 三种类型。

(1) 100BaseTX 采用 5 类非屏蔽双绞线，使用两对线对。

(2) 100BaseFX 采用多模光纤或单模光纤。

(3) 100BaseT4 采用 3 类非屏蔽双绞线，使用全部 4 对线对。

4．交换型以太网的中心设备是以太网交换器。交换型以太网系统与共享型以太网比较有如下优点。

(1) 每个端口上可以连接站点，也可以连接一个网段。不论站点和网段均独占该端口的带宽。

(2) 系统的最大带宽可以达到端口带宽的 *n* 倍，其中 *n* 为端口数。*n* 越大，系统的带宽越高。

(3) 交换器连接了多个网段，每一个网段都是独立的，被隔离的。但如果需要的话，独立网段之间通过其端口也可以建立暂时的数据通道。

(4) 被交换器隔离的独立网段上数据流信息不会随意广播到其他端口上去，因此具有一定的数据安全性。

5．

(1) 快速以太网和千兆位以太网属于高速以太网，是在 10Mb/s 以太网基础上发展起来的数据传输率更高的以太网技术。

(2) 快速以太网是在 10BaseT 和 10BaseF 技术基础上发展起来的具有 100Mb/s 数据传输率的以太网，快速以太网的传输媒体和媒体布局向下兼容 10Mb/s 以太网，帧结构和媒体访问控制方式则完全按照 IEEE 802.3 基本标准。

(3) 千兆位以太网是快速以太网的自然发展，只是数据传输率达到 1000Mb/s，二者的拓扑结构完全一致，传输媒体的媒体布局在快速以太网基础上有所发展，但向下兼容快速以太网和 10Mb/s 以太网，帧结构和媒体访问控制方式也与 IEEE 802.3 基本类同，但有所发展。

6．240Mb/s(24×10Mb/s)

7．

【问题 1】

(1) 只有链路上提供独立的发送和接收媒体的以太网产品才能支持全双工操作。

(2) 在 10Mb/s 以太网中只有 10BaseT 和 10BaseF 支持全双工操作。

(3) 在 100Mb/s 以太网中 100BaseTX、100BaseFX 都支持全双工操作。

(4) 在 1000Mb/s 以太网中 1000BaseLX、1000BaseSX、1000BaseCX、1000BaseTX 都支持全双工操作。

【问题 2】全双工以太网技术是用来说明以太网设备端口的传输技术，与传统半双工以太网技术区别在于：每个端口和交换机背板之间都存在两条逻辑通路。这样，每一个端口就可以同时接收和发送帧，不再受 CSMA/CD 的约束，在端口发送帧时不再会发生帧的碰撞，已无碰撞域的存在。这样一来，端口之间媒体的长度仅仅受数字信号在媒体上传输衰变的影响，而不像传统以太网半双工传输时还要受碰撞域的约束。

8．根据最小帧长度的计算公式：

$$L_{min}=\text{slot time}\times R\approx(2S/0.7C+2t_{PHY})\times R$$
$$=(2\times500/(0.7\times3\times10^{8})+2\times10^{-5})\times10\times10^{6}$$
$$=248(\text{位})$$

所以该网络最小帧长度为 248 位。

9.

【问题 1】收发器的主要功能有：向媒体发送信号、自媒体接收信号、识别媒体是否存在信号。

【问题 2】对于 10Mb/s 的以太网有 10Base5、10Base2、10BaseT、10BaseF 几种收发器。

【问题 3】集线器在以太网系统中具有的主要功能有：一是媒体上信号的再生和再定时，二是检测碰撞，三是端口的扩展功能，四是混合连接 10Base5 与 10Base2 以太网系统。

1.3 以太网交换机的部署

1.3.1 考点辅导

1.3.1.1 交换机的连接模式

交换机的连接模式有级联模式、堆叠模式和混合模式。

1. 级联模式

级联模式是最常规、最直接的一种扩展方式。级联模式是通过双绞线或光纤来级联，一般在交换机的前面板上有专门的级联口，如果没有，也可以用交叉线接法来级联。级联是通过端口进行的，级联后两台交换机是上下级的关系。

级联模式起源于早期的共享型集线器，其物理拓扑结构是星型的，而逻辑拓扑结构是总线型的。集线器仅相当于一条浓缩的总线，在集线器的某一个端口级联另一台集线器，只是相当于把浓缩的总线又加长了一些，但其仍然是一条总线，所有端口都要在一个碰撞域里受 CSMA/CD 的约束。但这样相当于把传输媒体加长了，在加长的传输媒体上又增加了一些端口。但付出的代价是，在这个碰撞域里，又多了一些端口共享整个带宽，从而导致网络性能低下。当然，这种级联方式必须遵循 5-4-3 法则，也就是级联不能超过 4 层。

在交换机上进行级联，级联交换机的端口共享的仅仅是被级联交换机端口的带宽，而不是整个网络的带宽。更何况目前的交换机级联通常是高速交换机级联低速交换机，即 1000Mb/s 端口级联 100/1000Mb/s 的交换机；100Mb/s 端口级联 10/100Mb/s 的交换机；或者是交换机级联共享型的集线器。由此一来，级联模式极大程度地克服了传统集线器级联共享带宽，而导致网络性能降低的弊端。

2. 堆叠模式

堆叠通常是为了扩充带宽用的，通常用专门的堆叠卡插在交换机的后面，用专门的堆叠电缆连接几台交换机，堆叠后这几台交换机相当于一台交换机。堆叠是采用交换机背板的叠加，使多个工作组交换机形成一个工作组堆，从而提供高密度的交换机端口，堆叠中的交换机就像一个交换机一样，配制一个 IP 地址即可。

级联是通过交换机的某个端口与其他交换机相连的，而堆叠是通过集线器的背板连接

起来的，它是一种建立在芯片级上的连接。如两个 24 口交换机堆叠起来的效果就像是一个 48 口的交换机。

常见的堆叠有两种：菊花链堆叠和矩阵堆叠。

3. 混合模式

在实际应用中，由于网络的复杂性、用户需求的多重性，通常同时使用两种模式进行交换机的部署，我们称其为混合模式。

1.3.1.2　以太网交换机的设置

对一台新的交换机进行配置和管理有两个主要步骤：一是通过仿真终端进行 IP 地址设置，二是通过浏览器进行管理。

1. 通过仿真终端进行 IP 地址设置

通过仿真软件设置 3COM 交换机 IP 地址的步骤如下。

(1) 用一条 RS-232 型电缆将管理终端的串口与交换机的控制台端口(Console)相连。

(2) 运行仿真终端软件，通常使用【附件】中的【超级终端】命令即可。

(3) 选择所连接的串口，如 COM1 端口。

(4) 根据说明书设置仿真终端的位率、数据位、奇偶校验和停止位等参数。

(5) 设置远程登录的用户名、密码及其他常见用户名。

(6) 设置 IP 地址及子网掩码。

2. 通过浏览器进行管理

(1) 打开浏览器，在 URL 栏中输入交换机 IP 地址后按 Enter 键，出现交换机的 Web 登录界面，在其中输入相应的用户名和密码后，单击【确定】按钮。

(2) 进入交换机的 Web 管理页面。

(3) 在 Web 管理页面中，既可以查看交换机的基本信息，也可以进行一些参数设置，如修改交换机管理用户的口令。

1.3.2　典型例题分析

例 1　以太网交换机一定要设置才能工作，是否正确？

分析：一台新的交换机部署到网络中后，使用默认配置就可以工作，不需要再进行设置。因为它是一种将软件装在 FlashMemory(闪存)中的硬件设备，当加电时，首先进行一系列自检，对所有的端口进行测试之后，交换机就处于工作状态。这时设备的交换表是空的，它可以通过自学来了解各个端口的设备连接情况，并将设备的 MAC 地址记录在交换表中，当有信息交换时，交换机就根据交换表来进行数据转发。

但是，当有一些高级应用和需求时，例如，通过交换机划分 VLAN，或是对交换机进行远程管理等，就需要对交换机进行设置。

答案：错误，以太网交换机在一般应用时，不需进行任何设置即可使用。

例 2　交换机之间级联只能采用双绞线，是否正确？采用什么类型的级联双绞线？

分析：交换机之间级联可通过双绞线或光纤。用双绞线进行级联时，可根据实际情况采用直通线或交叉线。

答案：错误。级联双绞线可根据需要采用直通线或交叉线。

例 3　非屏蔽双绞线的直通线和交叉线可用于下列哪两种设备间的通信？集线器到集线器(不使用级联端口)使用__(1)__；PC 到集线器使用__(2)__；PC 到交换机使用__(3)__；PC 到 PC 使用__(4)__。

分析：对于那些没有专用级联端口的集线器之间的级联，双绞线接头中线对的分布与连接网卡和集线器有所不同，必须要用交叉线。而许多集线器为了方便用户，提供了一个专门用来连接到另一台集线器的普通端口，对此类集线器进行级联时，双绞线均采用直通线。

答案：(1)交叉线　(2)直通线　(3)直通线　(4)交叉线

例 4　交换机与集线器(Hub)如何进行级联才能达到最佳效果？

分析：在 Hub 和交换机性能优化方面主要体现在 Hub 或交换机的级联上。如果需要 Hub 与 Hub 或 Hub 与交换机级联，则一定要注意 Hub 的带宽是所有端口共用的，因此每个端口实际利用的带宽则是应用总带宽(如 100Mb/s)除以所用端口数。所以一般不用 Hub 来级联，而是通过用 Hub 连接在交换机的端口上，因为交换机所指的带宽就是每个端口的实际可用带宽，如 n10Mb/s+m100Mb/s，就表明在这个交换机上有 n 个 10Mb/s 的带宽，有 m 个 100Mb/s 的带宽端口，这些带宽是具体端口独享的，而不受交换机所用端口数的限制。

也就是说，如果一个 Hub 连在一个交换机的 100Mb/s 端口上，则这个 Hub 上就拥有总共 100Mb/s 的带宽；如果一个 Hub 连接在有 100Mb/s 带宽的 Hub 端口上，则连接一个 Hub 可能使用了 10 个端口，实际上下一个 Hub 的总带宽就远达不到 100Mb/s 的带宽，这样就影响了连接在下一个 Hub 上的工作站速度。所以 Hub 级联一般最多为两层，层数多了会使速度呈倍差级数减慢。

另外还有两点要注意，其一是当 Hub 要通过交换机级联时最好连接在 100Mb/s 带宽的端口，除非没有 100Mb/s 端口可用了；其二是要注意双绞线最大单段网线长度在 100m 以内，否则信号会衰减严重，影响网络速度。

答案：一个 Hub 连在一个交换机的 100Mb/s 或 10Mb/s 端口上，同时相互级联的网线长度在 100m 之内。

1.3.3　同步练习

1. 什么是级联？
2. 简述级联的优势。
3. 常见的堆叠有哪两种？堆叠技术的最大优点是什么？
4. 简述堆叠模式的优、缺点。
5. 在网络中利用以太网交换机进行部署时，常采用哪三种模式？
6. 对没有任何设置的交换机通过何种方式进行配置？

7．设置了 IP 地址以后的交换机可采用哪两种方式进行远程管理？

8．描述通过仿真软件设置 3COM 交换机 IP 地址的步骤。

9．通过 Web 页面可对设置 IP 地址的 3COM 3300 交换机进行远程管理，请列举出通过远程管理可实现哪些功能？

1.3.4 同步练习参考答案

1．级联是通过双绞线或光纤把需要级联的设备通过端口相连接，从而达到增加同一网络端口数目的方法。

2．级联的优势如下。

(1) 级联模式可使用通用的以太网端口进行层次间互联，其中包括 100Mb/s 端口、1000Mb/s 端口以及新兴的 10Gb/s 端口。

(2) 级联模式是组建结构化网络的必然选择，级联使用普通的、长度限制并不严格的电缆(光纤)，各个级联单元的位置相对较随意，非常有利于综合布线。

(3) 级联模式通常是解决不同品牌的交换机之间以及交换机与集线器之间连接的有效手段。

3．常见的堆叠有两种：菊花链堆叠和矩阵堆叠。堆叠技术的最大的优点就是提供简化的本地管理，将一组交换机作为一个对象来管理。

4．堆叠模式的优点如下。

(1) 增加网络端口的同时，还增加了逻辑通道，扩充了网络带宽，不同堆叠单元的端口之间可以直接交换，进行快速转发，从而极大地提高了网络性能。

(2) 不受 5-4-3 法则的约束，堆叠单元可以超过 4 个。

(3) 提供简化的本地管理，将一组交换机作为一个对象来管理。

堆叠模式的缺点如下。

(1) 堆叠是一种非标准化技术，各个厂商之间不支持混合堆叠，同一组堆叠交换机必须是同一品牌。

(2) 堆叠模式不支持即插即用，在物理连接完毕之后，还要对交换机进行相应的设置，才能正常运行。

(3) 不存在拓扑管理，一般不能进行分布式布置。

5．采用三种模式：级联模式、堆叠模式和混合模式。

6．对没有任何设置的交换机通过仿真终端可设置交换机的登录用户名、密码、IP 地址及子网掩码等。

7．交换机可通过 Telnet 命令行的方式及 Web 页面的方式进行远程管理。

8．设置步骤如下。

(1) 用一条 RS-232 型电缆将管理终端的串口与交换机的控制台端口(Console)相连。

(2) 运行仿真终端软件如(超级终端)。

(3) 选择所连接的串口。

(4) 根据说明书设置仿真终端的位率、数据位、奇偶校验和停止位等参数。

(5) 设置远程登录的用户名、密码及其他常见用户名。

(6) 设置 IP 地址及子网掩码。

9．远程管理可实现如下功能：

(1) 可查看连入交换机机器网卡的 MAC 地址。

(2) 可查看每一个端口的状态。

(3) 可根据需要关闭、打开端口。

(4) 可以修改交换机管理用户的口令。

(5) 可根据需要对端口进行 VLAN 的划分等。

1.4 交换机与路由器的基本配置

1.4.1 考点辅导

1.4.1.1 交换机的基本配置

不同厂家生产的不同型号的交换机，其具体的配置命令和方法是有差别的。不过配置的原理基本都是相同的，本节主要以 Cisco Crystal 2950 系列交换机为例介绍交换机配置的基本技术和技能。

1. 电缆连接及终端配置

如图 1-19 所示，接好 PC 和交换机各自的电源线，在未开机的条件下，把 PC 的串口(COM 1)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。交换机 Console 端口的默认参数如下。

- 端口速率：9600b/s。
- 数据位：80。
- 奇偶校验：无。
- 停止位：1。
- 流控：无。

在配置 PC 的超级终端时只需将端口属性的配置和上述参数相匹配，就可以成功地访问到交换机。

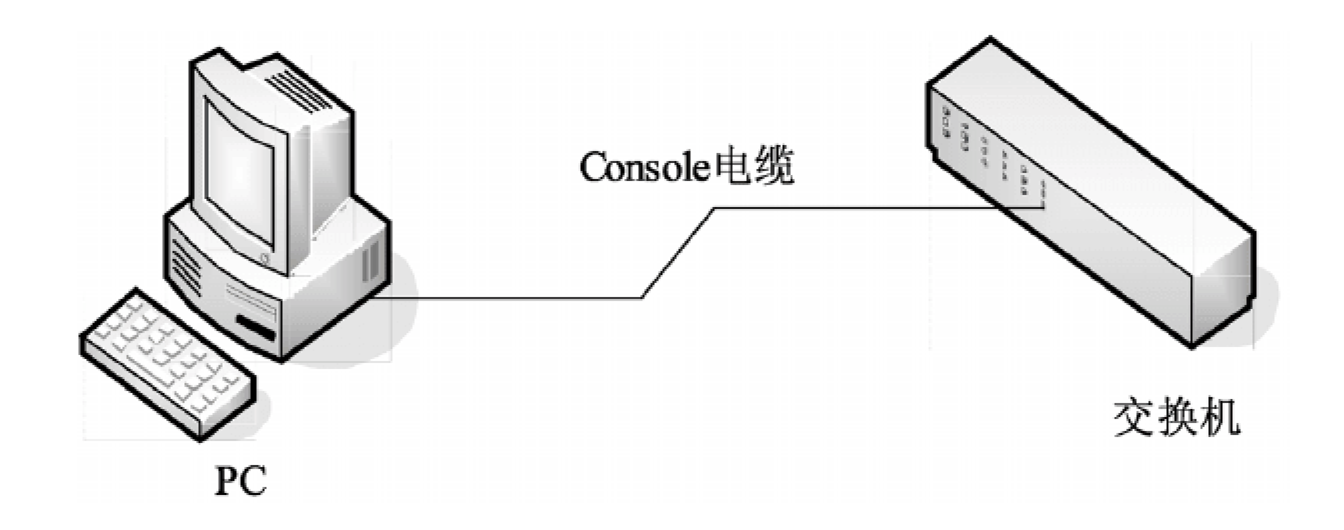


图 1-19 仿真终端与交换机的连接

2. 交换机的启动

在连接好线路，配置好超级终端仿真软件后，就可以打开交换机，此时超级终端窗口

就会显示交换机的启动信息。这些信息为用户提供了丰富的信息，利用这些信息，可以对交换机的硬件结构和软件加载过程有直观的认识。这些信息对我们了解该路由器以及对它作相应的配置很有帮助。另外，部件号、序列号、版本号等信息在产品验货时都是非常重要的信息。

3. 交换机的配置模式

交换机有以下常见的配置模式：普通用户模式、特权模式、全局配置模式和局部配置模式。在这些配置模式下，用户对交换机所具有的权限是不同的。在普通用户模式下，用户只能够对交换机进行简单的操作，如查询操作系统版本和系统时间，使用很少的几个命令；在特权模式下，用户可以使用较多的命令对交换机进行查看、配置等操作；在全局配置模式下，主要完成对交换机的配置，如虚拟局域网的配置、访问控制列表的配置等；在局部配置模式下，用户可以对某个具体端口进行配置。这几种配置模式是递进的关系。

(1) 普通用户模式。在交换机正常启动后，用户使用超级终端仿真软件或 Telnet 登录交换机，自动进入用户配置模式。其命令如下。

```
switch>
```

(2) 特权模式。在用户模式下，输入以下命令可以进入特权模式。

```
switch>enable
switch#
```

(3) 全局配置模式。在特权模式下，输入以下命令可以进入全局配置模式。

```
switch>config terminal
switch(config)#
```

(4) 局部配置模式。它包括端口配置模式和线路配置模式。在全局配置模式下，输入以下命令可以进入局部配置模式。

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#            (端口配置模式)
switch(config)#line console 0
switch(config-line)#           (线路配置模式)
```

4. 交换机的基本配置

在默认配置下，所有接口处于可用状态并且都属于 VLAN 1，这种情况下交换机就可以正常工作了。但为了方便管理和使用，首先应对交换机进行基本的配置。最基本的配置可以通过启动时的对话框配置模式完成，也可以在交换机启动后再进行配置。

(1) 配置 enable 口令和主机名。

```
Switch>                                (用户执行模式提示符)
Switch >enable                         (进入特权模式)
Switch#                                (特权模式提示符)
Switch #config terminal                (进入全局配置模式)
Switch(config)#                        (全局配置模式提示符)
Switch(config)#enable password cisco   (设置 enable password 为 cisco)
Switch(canfig)#enable secret ciscol    (设置 enable secret 为 ciscol)
```

```
Switch(config)#hostname C2950              (设置主机名为 C2950)
C2950{config}#end                          (退回到特权模式)
```

(2) 配置交换机 IP 地址、默认网关、域名、域名服务器。

```
C2950(config)#ip address 192.168.1.1 255.255.255.0     (设置交换机 IP 地址)
C2950(config)#ip default-gateway 192.168.1.254         (设置默认网关)
C2950(config)#ip domain-name cisco.com                 (设置域名)
C2950(config)#ip name-server 200.4.0.1                 (设置域名服务器)
```

(3) 配置交换机的端口属性。

```
 C2950(config)#interface FastEtheraet0/1        (进入接口 0/1 的配置模式)
 C2950(config-i)#speed?                         (查看 speed 命令的子命令)
 10   Force 10Mbps   operation                  (显示结果)
100  Force 100Mbps  operation
suto  Enable AUTO speed  configuration
 C2950(config-if) #speed 100                    (设置该端口速率为 100Mbps)
 C295Q(config-if) #duplex?                      (查看 duplex 命令的子命令)
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half- duplex operation
C2950(config-if)#dupleax full                   (设置该端口为全双工)
C2950(config-if)#description  TO_PC1            (设置该端口描述为 TO PC1)
C2950(config-if)#^Z                             (返回到特权模式，同 end)
C2950#show interface FastEthernet0/1            (查看端口 on 的配置结果)
C2950#show interface FastEthernet0/l status     (查看端口 0/1 的状态)
```

(4) 配置和查看 MAC 地址表。

```
C2950(config)#mac-address-table?          (查看 mac-address-table 的子命令)
C2950(config)#mac-address-table aging-time 100       (设置超时时间为 100s)
C2950(config)#mae-address-table permanent 0000.0c01.bbcc f0/3
                                          (加入永久地址)
C2950(config)#mae-address-table restricted static 0000.0c02.bbcc f0/6 f0/
                                          (加入静态地址)
C2950(config)#end
C2950#sbow mao-address-table              (查看整个 MAC 地址表)
```

1.4.1.2 配置和管理 VLAN

VLAN(Virtual Local Area Network)的中文名称为“虚拟局域网”，VLAN 是为了解决以太网广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态地管理网络。

VLAN 技术是交换技术的重要组成部分，也是交换机的重要进步之一。它用以把物理上直接相连的网络从逻辑上划分为多个子网。每一个 VLAN 对应一个广播域，处于不同 VLAN 上的主机不能进行通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置和管理主要涉及 VTP、VLAN 中继和 VLAN 的配置。

1. 划分 VLAN 的方法

虚拟局域网是交换机的重要功能，通常虚拟局域网的实现形式有三种，即静态端口分配、动态虚拟网和多虚拟网端口配置。

静态虚拟网的划分通常是网管人员使用网管软件或直接设置交换机的端口，使其直接从属于某个虚拟网。这些端口一直保持这些从属性，除非网管人员重新设置。这种方法虽然比较麻烦，但比较安全，容易配置和维护。

支持动态虚拟网的端口，可以借助智能管理软件自动确定它们的从属。端口是通过借助网络包的 MAC 地址、逻辑地址或协议类型来确定虚拟网的从属。一旦网管人员配置好后，用户的计算机就可以灵活地改变交换机端口，而不会改变该用户的虚拟网从属性。

多虚拟网端口配置支持一用户或一端口可以同时访问多个虚拟网。

静态虚拟网是最普遍使用的一种划分 VLAN 的方法，但会带来安全上的隐患。

2. 配置 VTP 协议

VTP 协议可以帮助交换机设置 VLAN。VTP 协议可以维护 VLAN 信息全网的一致性。VTP 有三种工作模式，即服务器模式、客户模式和透明模式。其中服务器模式可以设置 VLAN 信息，服务器会自动将这些信息广播到网上其他交换机以统一配置；客户模式下交换机不能配置 VLAN 信息，只能被动地接受服务器的 VLAN 配置；而透明模式下是独立配置，它可以配置 VLAN 信息，但是不广播自己的 VLAN 信息，同时它接收到服务器发来的 VLAN 信息后并不使用，而是直接转发给别的交换机。

配置 VTP 协议的命令如下：

```
vlan database             (进入 VLAN 配置子模式)
vtp domain vname          (设置 VTP 管理域名称)
vtp server|client         (设置交换机为服务器(或者客户端)模式)
vtp pruning               (启动修剪功能)
```

3. 配置 VLAN Trunk 端口

VLAN Trunk(VLAN 中继)也称为 VLAN 主干，是指在交换机与交换机或交换机与路由器之间连接的情况下，在互相连接的端口上配置中继模式，使得属于不同 VLAN 的数据帧都可以通过这条中继链路进行传输。

配置 VLAN Trunk 端口的命令如下：

```
interface fa0/1                      (进入端口配置模式)
switchport mode truck                (设置当前端口为 Trunk 模式)
switchport trunk allowed vlan all    (设置允许从该端口交换数据的 VLAN)
```

4. 创建 VLAN

VLAN 信息可以在服务器模式或透明模式交换机上创建。创建 VLAN 的命令如下：

```
valn a_num mod_num/port_num          (创建 VALN)
clear vlan a_num                     (清除一个已存在的 VALN)
```

5. 将端口加入到某个 VLAN 中

配置完 VTP 协议及 VLAN Trunk 端口后就可以设置将端口归属于哪个 VLAN 了。将端

口加入到某个 VLAN 中的命令如下：

```
switchport access vian 2                    (把端口分配给相信的 VLAN2 )
```

1.4.1.3 路由器的配置

1. 路由器的基本配置

与交换机的配置类似，路由器的配置操作有以下几种模式：普通用户模式、特权模式和配置模式。在用户模式下，用户只能发出有限的命令，这些命令对路由器的正常工作没有影响；在特权模式下，用户可以发出丰富的命令，以便更好地控制和使用路由器；在配置模式下，用户可以创建和更改路由器的配置。

配置路由器的连接方式如图 1-20 所示，使用专用的配置线缆将路由器的 Console 端口(配置端口)与计算机的串行口(RS232 接口)相连，然后打开计算机中的超级终端进行连接。主机名及路由器口令的设置和 1.4.1.1 节中交换机配置的主机名及口令相同。

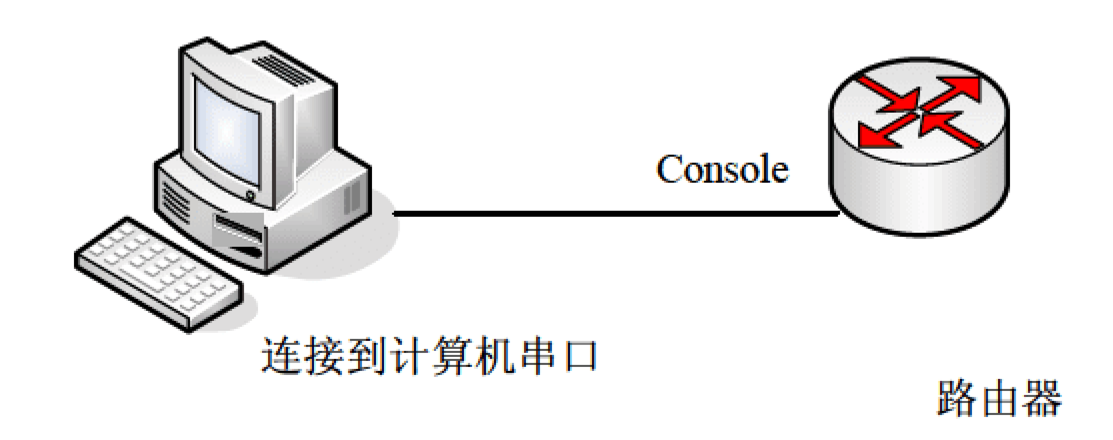


图 1-20 配置路由器的连接方式

配置路由器以太网接口：路由器一般提供一个或多个以太网接口槽，每个槽上会有一个以上以太网接口。以太网接口也因此而命名{Ethernet 槽位端口}或{FastEthernet 槽位/端口}。比如，FastEthernet0/0、FastEthernetl1/1，也可缩写为 F0/0、F1/1。

以 Cisco2600 系列交换机为例，连接好仿真终端到路由器的 Console 电缆线后，就可以对路由器进行初始的配置工作了。配置以太网接口的命令如下：

```
Router>enable                                    (进入特权执行模式)
Router #config t                                 (进入全局配置模式)
Enter configuration commands, one per line.  End with CNTLIZ.
Router (config)#interface FastEtbernet0/1  (进入接口 F0/1 配置模式)
Router (config-if)#ip address 192.168.1.11 255.255.255.0  (设置接口 IP 地址)
Router (config-if)#no shutdown                  (激活接口)
10:05:01 %LINK-3-UPDOWN:Interface FastEthernet010, changed state to up
Router (config-if)#end                          (退回到特权模式)
Router#show running-config                      (检查配置结果)
```

2. 静态路由的配置

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径，在网络结构比较简单，且一般到达某一网络所经过的路径惟一的情况下采用静态路由。静态路由的配置命令如下：

```
router(config)# ip route <network.> [mask] {address|interface} [distance]
[permanent]
```

其中，network 是目的网络的网络地址；mask 是网络地址子网掩码；address 是下一跳 IP 地址；interface 是本端接口号码；distance 是管理距离，默认是 1；permanent 表示这个路径是永远存在的。

1.4.1.4　配置路由协议

距离矢量(Distance Vector)路由协议计算网络中所有链路的矢量和距离并以此为依据确认最佳路径。使用距离矢量路由协议的路由器定期向其相邻的路由器发送全部或部分路由表。典型的距离矢量路由协议有 RIP 和 OSPF。

下面我们将分别讨论如何在路由器中配置 RIP 和 OSPF 动态路由协议。

1. 配置 RIP 协议

RIP 使用非常广泛，它简单、可靠，便于配置。RIP 版本 2 还支持无类域间路由(ClasslessInter-Domain Routing，CIR)和可变长子网掩码(Variable Length Subnetwork Mask，VLSM)和不连续的子网，并且使用组播地址发送路由信息。但是 RIP 只适用于小型的同构网络，因为它允许的最大跳数为 15，任何超过 15 个站点的目的地均被标记为不可达。RIP 每隔 30s 广播一次路由信息。

1)　相关配置命令

```
router rip                (进入 RIP 协议配置子模式)
version 1/2               (设置 RIP 协议版本 1/2)
network  network          (声明指定与该路由器相连的网络)
```

2)　相关调试命令

```
show ip route             (显示路由信息)
show ip protocol          (显示协议信息)
```

用 show ip route 命令显示出某路由信息如下：

```
R: 192.168.3.0 [120/1] via 192.168.69.1, 00:00:24, Serial0
```

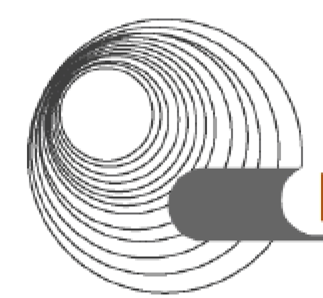
对路由表中的项目解释如下。

- R：表示此项路由是由 RIP 协议获取的。
- 192.168.3.0：表示目标网段。
- [120/1]：120 表示 R1P 协议的管理距离默认为 120，1 是该路由的度量值，即跳数。
- Via：经由的意思。
- 192.168.69.1：表示从当前路由器出发到达目标网的下一跳点的 IP 地址。
- 00:00:24：表示该条路由产生的时间。
- Serial0：表示该条路由使用的接口。

2. 配置 OSPF 协议

开放最短路径优先(Open Shortest Path First，OSPF)协议是重要的路由选择协议。它是一种链路状态路由选择协议，是由 Internet 工程任务组开发的内部网关(Interior Gateway Protocol，IGP)路由协议，用于在单一自治系统(Autonomous System，AS)内决策路由。

配置 OSPF 协议的相关命令如下：




```
router ospf process-id1                          (指定使用 OSPF 协议)
network address wildcard-mask area area-id2      (指定与该路由相连的网络)
neighbor ip-address                              (指定与该路由相邻的节点地址)
```

1.4.2　典型例题分析

例 1　阅读以下技术说明，根据要求回答问题 1～问题 4。

【说明】

图 1-21 是 VLAN 配置的结构示意图。

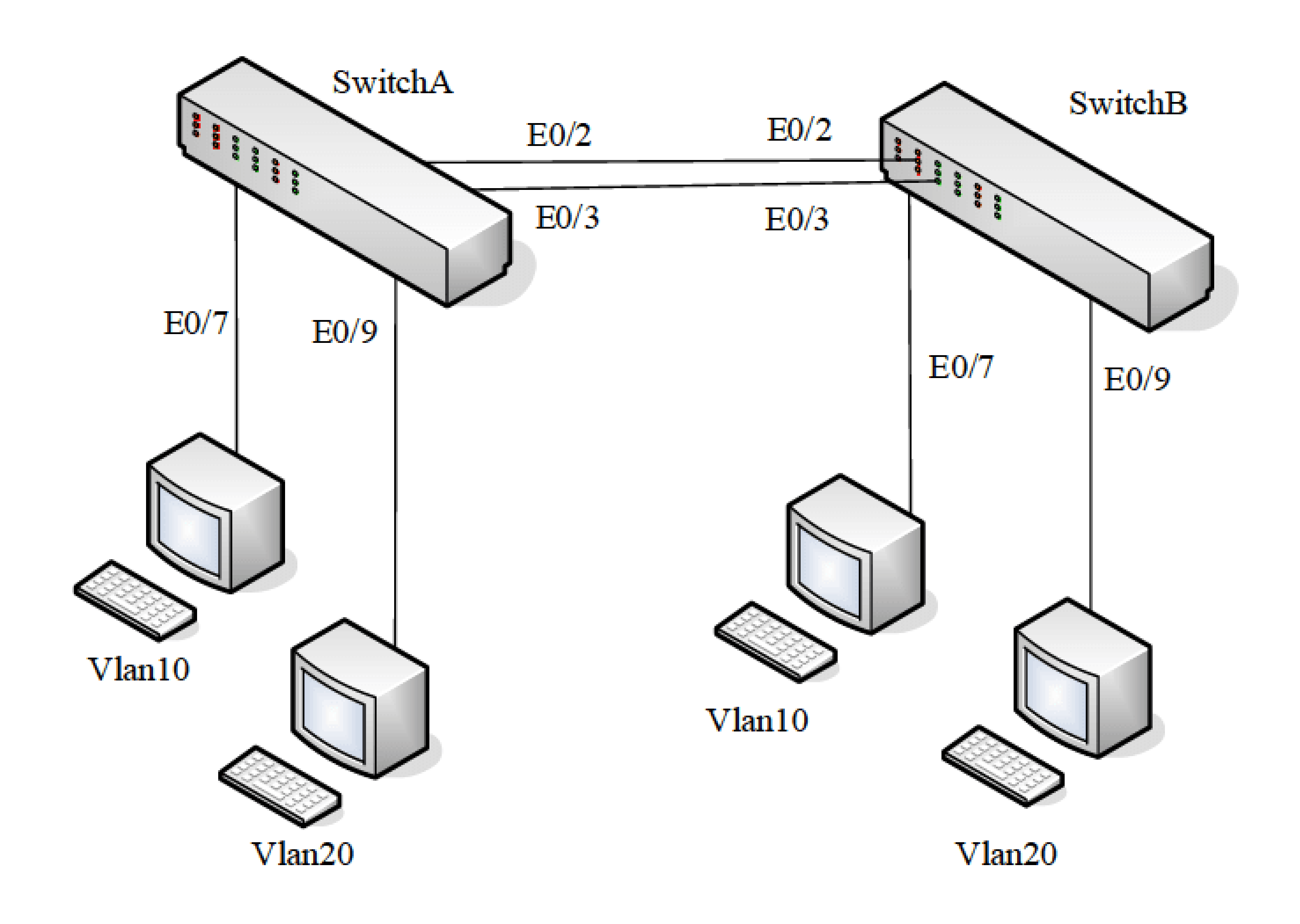


图 1-21　某 VLAN 配置的拓扑结构

【问题 1】(5 分)

请阅读下列关于 SwitchA 的配置信息，并在(1)～(5)处解释相应语句的作用。

```
SwitchA> enable                        (进入特权模式)
Switch# config terminal                (进入配置模式)
Switch(config)# hostname SwitchA       ____(1)____
SwitchA(config)# end
SwitchA#
SwitchA# vlan database                 ____(2)____
SwitchA(valn)# vtp server              ____(3)____
SwitchA(valn)# vtp domain vtpserver    ____(4)____
SwitchA(valn)# vtp pruning             ____(5)____
SwitchA(valn)# exit                    (退出 VLAN 配置模式)
```

【问题 2】(2 分)

下面是交换机完成 Trunk 的部分配置，请根据题目要求，完成下列配置。

```
SwitchA(config)# interface f0/3                     (进入端口 3 配置模式)
SwitchA(config-if)# switchport____(6)____           (设置当前端口的 Trunk 模式)
SwitchA(config-if)# switchport trunk ____(7)____    (设置允许所有 Vlan 通过)
SwitchA(config-if)# exit
```

```
SwitchA(config)# exit
Switch#
```

【问题 3】(4 分)

下面是交换完成端口配置的过程，请根据题目要求，完成下列配置。

```
Switch(config)# interface f0/7          (进入端口 7 配置模式)
Switch(config-if)# ____(8)____          (设置端口为静态 VLAN 访问模式)
Switch(config-if)# ____(9)____          (把端口 7 分配给 VLAN10)
Switch(config-if)# exit
Switch(config)# exit
```

【问题 4】(2 分)

基于交换机端口的 VLAN 划分方法属于 (10) 。

A.　动态 VLAN 实现方式　　　　　　　　B.　静态 VLAN 实现方式

【问题 5】(2 分)

在 VLAN 中，STP 是指 (11) 协议，VTP 是指 (12) 协议。

分析：

【问题 1】

本题要求考生掌握 VTP 配置的命令解释。对于(1)空缺，由它所在命令行的交换机配置模式“Switch(config)#”和下一行“SwitchA(config)#”的不同可知，配置语句 hostname SwitchA 的作用是将该交换机的主机名修改为 SwitchA；对于(2)空缺，由它所在命令行的交换机配置模式“SwitchA#”和下一行“SwitchA(valn)#”的不同可知，配置语句 Vlan database 的作用是进入该交换机的 VLAN 配置子模式；在交换机的 VLAN 配置子模式中，(3)空缺处的命令行的配置语句为 vtp server，其作用是设置该交换机的 VTP 模式为 Server 模式；(4)空缺处所在命令行的配置语句为 vtp domain vtpserver，其作用是设置该交换机的 VTP 管理域名为 vtpserver；(5)空缺处所在命令行的配置语句为 vtp pruning，其作用是启动该交换机的 VTP 修剪功能。

【问题 2】

本题要求考生掌握交换机 VLAN Trunk 端口配置的实践操作过程。解答思路如下。

① 跨交换机的同一 VLAN 内的数据经过 Trunk 线路进行交换，在默认情况下 Trunk 允许所有的 VLAN 通过。

② 配置语句 interface f0/3 使得交换机从配置模式进入到快速以太网端口 3 的配置模式。根据(6)空缺处所在命令行后面的解释信息“设置当前端口为 Trunk 模式”可知，(6)空缺处完整的配置语句是 switchport mode trunk。

③ 根据(7)空缺处所在命令行后面的解释信息“设置允许所有 Vlan 通过”可知，(7)空缺处完整的配置语句是 switchport trunk allowed vlan all。

【问题 3】

本题要求掌握将交换机某端口添加到某个 VLAN 中的实践操作过程。

由于交换机出厂配置的工作状态是服务器模式，系统自动创建一个 VLAN(即 VLAN1)默认将所有的端口都归属到这个 VLAN 内。因此，在交换机中配置 VLAN 时，VLAN1 不

能被创建、删除或重命名。

在基于端口的 VLAN 划分中，交换机上的每一个端口允许以 access、multi、trunk 3 种模式划入 VLAN 中。其中，对于 access 模式，端口仅能属于一个 VLAN，只能接受没有封装的帧；对于 multi 模式，端口可以同时属于多个 VLAN，但只能接受没有封装的帧；对于 trunk 模式，该端口可以接收包含所属 VLAN 信息的封装帧，同时允许不同设备的相同 VLAN 通过 trunk 互连。

配置语句 interface f0/7 使得交换机从配置模式进入到快速以太网端口 7 的配置子模式。根据(8)空缺处所在命令行后面的解释信息“设置端口为静态 VLAN 访问模式”可知，(8)空缺处所填写的配置语句是 switchport mode access。

根据(9)空缺处所在命令行后面的解释信息“把端口 7 分配给 VLAN10”可知，(9)空缺处所填写的配置语句是 switchport access vlan10。

【问题 4】

这是一道要求掌握静态和动态 VLAN 基本知识及其特点的问答题。本题所涉及的知识点如下。

静态 VLAN 划分是创建 VLAN 最常用的方法。形成静态 VLAN 的过程是将交换机端口强制性地分配给某个 VLAN 的过程，即先在交换机上建立 VLAN，指定其基本参数(如 VTP 域、VLAN ID 等)，然后将交换机的每个端口分配给相应的 VLAN。在没有人为地修改该端口之前，该端口一直属于某一个 VLAN。不管是哪种网络设备接入该端口，它所归属的 VLAN 都不会改变。这种划分方式是基于端口来划分的，容易实现和监视，且比较安全，但是设置烦琐(每个端口都要设置)，并且 VLAN 的变化不灵活。如果想要改变某个端口的 VLAN，必须手动修改交换机配置。基于交换机端口的 VLAN 划分方法属于静态 VLAN 实现方式。

动态 VLAN 的配置可以基于网络设备的 MAC 地址、IP 地址、应用协议来实现。在动态方式中，管理员必须先建立一个较复杂的数据库，例如，输入要连接的网络设备的 MAC 地址及相应的 VLAN 号。当网络设备连接到交换机端口时，交换机自动把这个网络设备所连接的端口分配给相应的 VLAN。实现动态 VLAN 时，一般使用管理软件来进行管理。这种划分方式的特点是：VLAN 的变化很灵活，初始化配置后就不用关心用户接入哪个具体端口，但是要维护一个全网的数据库表，而且每次新用户加入时都需要进行较复杂的手工配置，即初始化配置的工作量较大。

【问题 5】

这是一道要求掌握 STP 和动态 VTP 含义及其作用的简答题。本题所涉及的知识点如下。

在交换机配置中，生成树协议(STP)是一个既能够防止环路又能够提供冗余线路的二层管理协议。为了使交换网络正常运行，STP 网络上的任何两个终端之间只有一条有效路径，即能暂时切断网络中的环路，在网络的环路消失之后，又能自动打开关闭的端口，从而保证网络不会中断。STP 使用生成树算法来求解无环路网络的最佳路径，使一些备用路径处于阻塞状态。大型交换网络中尤其是有多个 VLAN 的时候，配置 STP 很重要。STP 操作对于终端来说是透明的，而终端不管它们连在 VLAN 的一个部分或者多个部分。

VLAN 中继协议可以保持网络中 VLAN 配置的一致性，即在 VTP 域的某台交换机中增

加、删除和调整 VLAN 时，VTP 会自动地把交换机的 VLAN 变化信息向网络中其他的交换机广播，使得整个网络中同一个 VTP 域中的所有交换机同步地知道网络中其他交换机的 VLAN 变化信息，从而保持全网中交换机 VLAN 信息的自动同步。同时，VTP 还可以减少那些可能导致安全问题的配置。

答案：

【问题 1】

(1) 修改主机名为 SwitchA

(2) 进入 VLAN 配置子模式

(3) 设置本交换机为 Server 模式

(4) 设置 VTP 管理域名为 vtpserver

(5) 启动修剪功能

【问题 2】

(6) mode trunk (7) allowed vlan all

【问题 3】

(8) switchport mode access (9) switchport access vlan 10

【问题 4】

(10) B

【问题 5】

(11) 生成树 (12) VLAN 中继

1.4.3 同步练习

阅读以下技术说明，根据要求回答问题 1～问题 4。

【说明】

某单位内部网络拓扑结构如图 1-22 所示。

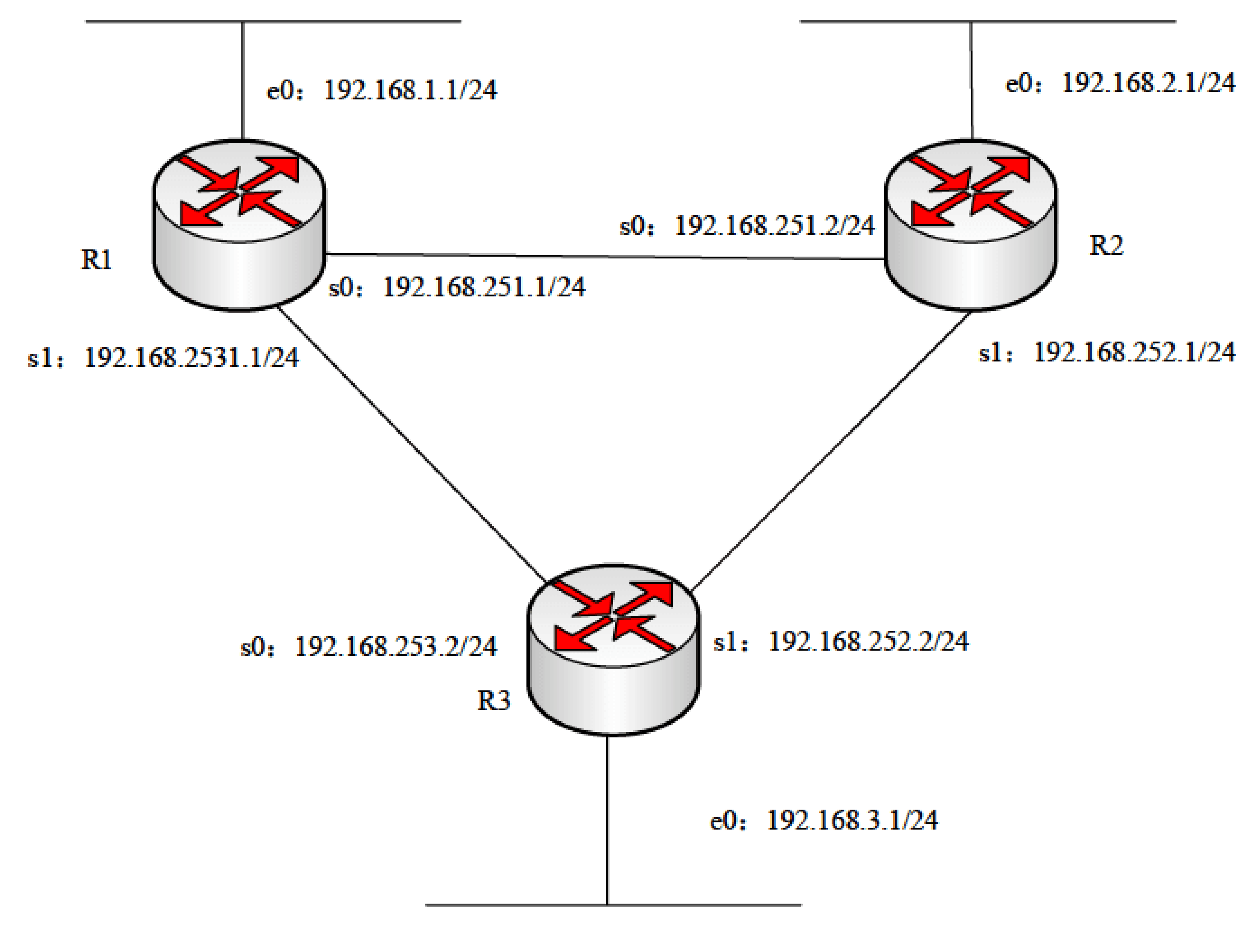
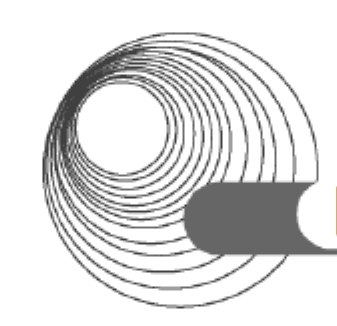


图 1-22 某单位内部网络拓扑结构



【问题 1】(2 分)

路由器第一次设置时，必须通过 Console 端口连接运行终端仿真软件的计算机进行配置，此时，终端仿真程序设置的波特率为___(1)___b/s。

【问题 2】(4 分)

路由器有多种配置模式，请根据以下命令提示状态，判断路由器处于何种配置模式下。

```
Router(Config) #                  (2)
Router >                          (3)
Router #                          (4)
Router(Config-if) #               (5)
```

【问题 3】(5 分)

以下是路由器 R1 的部分配置，请完成其配置，或者解释配置命令的含义。

```
R1(Config) #interface Fastethernet0
R1(Config-if) # ip address   (6)      (7)
R1(Config-if) #   (8)
!
R1(Config) #interface serial0
R1(Config-if) # ip address   (9)          (10)
```

【问题 4】(4 分)

为保证路由器的安全，网络管理员进行了如下设置，请在(11)~(13)处填写对应行语句的作用。

```
outer(Config) #no ip http server                       (11)
outer(Config) #snmp-server community admin RW          (12)
outer(Config) #access-list permit 192.168.5.1
Router(Config) #line con 0
Router(Config-line) #transport input none
Router(Config-line) #login local
Router(Config-line) #exec-timeout 5 0
Router(Config-line) #access-class 1 in                 (13)
```

1.4.4 同步练习参考答案

【问题 1】

(1) 9600

【问题 2】

(2) 全局配置模式　(3) 用户模式

(4) 特权模式　(5) 接口配置模式

【问题 3】

(6) 192.168.1.1　(7) 255.255.255.0　(8) no shutdown

(9) 192.168.251.1　(10) 255.255.255.0

【问题 4】

(11) 禁止以非加密的 HTTP 方式访问路由器，或路由器禁止 HTTP 服务

(12) 配置路由器具有读写权限的团体名为 admin

(13) 设置 ACL 允许 192.168.5.1 访问 Console0 端口

1.5　综 合 布 线

1.5.1　考点辅导

1.5.1.1　综合布线系统概述

1. 综合布线系统的概念

综合布线系统(PDS)是专为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。

综合布线系统具体的应用对象主要是通信和数据交换，即语音、数据、传真、图像信号。综合布线系统是一套综合系统，它可以使用相同的线缆、配线端子板、插头及模块插孔，解决传统布线存在的兼容性问题。综合布线系统是智能化大厦工程的重要组成部分，是智能化大厦传送信息的神经中枢。

2. 综合布线系统的特点

与传统布线系统相比，综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性等特点。

1)　兼容性

兼容性是指其设备可以用于多种系统。它将语音、数据信号的配线统一设计规划，采用统一的传输线、信息插接件等，把不同信号综合到一套标准布线系统中，同时，该系统比传统布线系统简捷很多，不存在重复投资，可以节约大量资金。

2)　开放性

综合布线系统由于采用开放式体系结构，符合国际标准，对现有著名厂商的硬件设备均是开放的，对通信协议也同样是开放的。

3)　灵活性

综合布线系统中每条线路均可传送语音、传真和数据，所有系统内的设备(计算机、终端、网络集散器、集线器或中心集线器、电话、传真)的开通及变动无须改变布线，只要在设备间或管理间作相应的跳线操作即可。

4)　可靠性

综合布线系统全部使用物理星型拓扑结构，任何一条线路有故障都不会影响其他线路，从而提高了可靠性。各系统采用同一传输介质，互为备用，又提高了备用冗余。

5)　经济性

综合布线系统设计信息点时要求按规划容量留有适当的发展容量，因此，就整体布线

系统而言，按规划设计所做的经济分析表明，综合布线系统会比传统布线系统的性价比更优，后期运行维护及管理费也会下降。

6) 先进性

为了适应数据传递、语音及多媒体技术的发展，综合布线系统采用双绞线与光纤混合布置方式进行布线。

3. 综合布线标准

综合布线标准有以下几种。

- 《建筑与建筑群综合布线系统工程设计规范》(国家标准 GB 30511—2000)。
- 《建筑与建筑群综合布线系统工程施工和验收规范》(国家标准 GB 30512—2000)。
- 《大楼通信综合布线系统第一部分总规范》(YD/T 926.1—2001)。
- 《大楼通信综合布线系统第二部分综合布线用电缆光纤技术要求》(YD/T 926.2—2001)。
- 《大楼通信综合布线系统第三部分综合布线用连接硬件技术要求》(YD/T 926.3—2001)。
- 《商用建筑通信布线标准》(北美标准 ANSI/TIA/EIA 568B)。
- 《信息技术——用户通用布线系统》(第 2 版)(国际标准 ISO/IEC 11801)。
- 《国际电子电气工程师协会：CSMA/CD 接口方法》(IEEE 802.3)。

4. 综合布线系统的构成

综合布线系统由 6 个子系统组成，即水平子系统、垂直子系统、工作区子系统、管理子系统、设备间子系统及建筑群子系统。大型布线系统需要用铜介质和光纤介质将 6 个子系统集成在一起。

(1) 水平子系统：由信息插座、配线电缆或光纤、配线设备和跳线等组成，又称为配线子系统。

(2) 垂直子系统：由配线设备、干线电缆或光纤、跳线等组成，又称为干线子系统。

(3) 工作区子系统：需要终端设备的独立区域。

(4) 管理子系统：是针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统：是安装各种设备的场所。对综合布线而言，还包括安装的配线设备。

(6) 建筑群子系统：由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

1.5.1.2 综合布线系统设计

1. 系统设计原则

在进行综合布线系统设计时通常应遵循以下原则。

(1) 采用模块化设计，易于在配线上扩充和重新组合。

(2) 采用星型拓扑结构，从而使系统扩充和故障分析变得十分容易。

(3) 应满足通信自动化与办公自动化的需要，即满足语音与数据网络的广泛要求。

(4) 确保任何插座互连主网络，尽量提供多个冗余互连信息点插座。

(5) 适应各种符合标准的品牌设备互联入网，满足当前和将来网络的要求。

(6) 电缆的铺设与管理应符合综合布线系统的设计要求。

2. 工作区子系统设计

工作区子系统提供从水平子系统的信息插座到用户工作站设备之间的连接，它包括工作站连线、适配器和扩展线等。

一部电话机或一台计算机终端设备的服务面积可按 8～10m^2 设置，也可按用户要求设置。采用标准信息插座，型号为 RJ-45，采用 8 芯连线，全部按标准制造，符合 ISDN 标准。在 RJ-45 插座内不仅可以插入数据通信通用的 RJ-45 接头，也可以插入电话机专用的 RJ-12 插头。

信息插座通常有 3 种安装形式：信息插座安装于地面上，信息插座安装于分隔板上，信息插座安装于墙上。如果安装于墙上，信息插座应放置在距地面 30～50cm 处。

3. 水平子系统设计

水平子系统是将垂直子系统线路延伸到用户工作区，由工作区的信息插座、信息插座至楼层配线设备(FD)的配线电缆或光纤、楼层配线设备和跳线等组成。

水平子系统的设计应按以下要求进行。

(1) 水平子系统一般应使用 20 年左右，通常采用管线敷设，这也对双绞线的性能和质量提出了更高的要求。

(2) 进行网络布线时应考虑未来的发展(信息点冗余及网络带宽的需求)。

(3) 水平子系统采用 4 对双绞线，通常在超 5 类和 6 类之间选择，在高速率应用场合宜采用光缆。

(4) 根据整个综合布线系统的要求，应在交换间或设备间的配线设备上进行连接，以构成电话、数据传输设备并进行管理，配线电缆宜采用双绞线。电缆长度应在 90m 以内。

4. 垂直子系统设计

垂直子系统主要用于连接各层配线室，并连接主配线室。

设计要求如下。

(1) 为安装和固定垂直子系统的电缆，要求建筑物竖井中应立有金属线槽，且每隔 2m 焊一根粗钢筋。

(2) 竖井中的线槽与各层配线室之间应有金属线槽连通。

(3) 垂直子系统采用的介质大多数为双绞线电缆和光纤。

5. 管理子系统设计

管理子系统由交连、互连配线架组成，为连接其他子系统提供手段。

设计要求如下。

(1) 根据信息点的数量，对于信息点不是很多的楼层，为便于管理，几个楼层可共用一个子配线间；对于有较多信息点的楼层，一个楼层设置一个配线间。

(2) 配线间的位置可选在弱电井附近的房间内。配线室设标准机柜，用于安装配线架(双绞线、光纤)和计算机网络通信设备。

6. 设备间子系统设计

设备间子系统(主配线间)由设备间中的电缆、连接器和相关支撑硬件组成，它把公共系统设备的各种不同设备互连起来。该子系统将中继线交叉连接处和布线交叉处与公共系统设备(如PBX)连接起来。

设计要求如下。

(1) 通常主配架设置在程控机房内，用于垂直光缆和PABX的连接。建议采用QCBIX系列配线架，可充分满足语音通信的要求。

(2) 通常计算机网络主配线架设在网管中心，使用光纤配线架，用来连接来自各分配线间的光纤，并通过光纤跳线和计算机网络中心交换机相连。光纤配线架可直接安装在标准的19in机柜内，用于主干光纤和网络设备的连接，十分易于管理。

(3) 对于设备间的建设应满足一定的要求，如室温、湿度、地板负重能力、消防、电源及UPS等。

7. 建筑群子系统设计

建筑群子系统应由连接各建筑物之间的综合布线缆线、建筑群配线设备(CD)和跳线等组成。

设计要求如下。

(1) 建筑物间的缆线宜采用地下管道或电缆沟的铺设方式。

(2) 建筑物群干线电缆、光缆、公用网和专用网电缆、光缆(包括天线馈线)进入建筑物时，都应设置引入设备，并在适当位置转换为室内电缆、光纤。引入设备还包括必要的保护装置。引入设备宜单独设置房间，如条件合适也可与BD或CD合设。引入设备的安装应符合相关规定。

(3) 建筑群和建筑物的干线电缆、主干光缆布线的交接不应多于两次。

(4) 从楼层配线架(FD)到建筑群配线架之间只应通过一个建筑物配线架(BD)。

8. 管线设计

综合布线系统中管线设计通常采用两种方案：装配式槽形电缆桥架、地面线槽走线。

9. 电气防护、接地及防火设计

综合布线系统应根据环境条件选用相应的缆线和配线设备，或采取防护措施，并应符合下列规定。

(1) 当综合布线区域内存在干扰或用户对电磁兼容性有较高要求时，宜采用屏蔽缆线和屏蔽配线设备进行布线，也可采用光纤系统。采用屏蔽布线系统时，所有屏蔽层应保持连续性。

(2) 综合布线系统采用屏蔽措施时，必须有良好的接地系统。

(3) 当电缆从建筑物外面进入建筑物时，电缆的金属护套或光纤的金属件均应有良好的接地，同时要采用过压、过流保护措施，并符合相关规定。

(4) 根据建筑物的防火等级和对材料的耐火要求，综合布线应采取相应的措施。

(5) 当综合布线线路上存在干扰源，且不能满足最小净距要求时，宜采用金属管线进行屏蔽。综合布线电缆与附近可能产生高平电磁干扰的电动机、电力变压器等电气设备之

间应保持必要的间距。墙上铺设的综合布线电缆、光纤及管线与其他管线应保持适当的间距。

1.5.1.3　综合布线系统的性能指标及测试

1. 双绞线系统的测试元素及标准

1)　连接图

连接图用于显示双绞线的详细情况。连接图测试通常是一个布线系统的最基本测试，因而对于 3～5 类布线系统都要求连接图测试。

2)　线缆长度

3～5 类布线系统都要求对线缆长度的准确测试。对线缆长度要求如下：基本回路线缆长度不大于 94m(包括测试跳线)，通道回路线缆长度不大于 100m(包括设备跳线和快接式跳线)。

3)　衰减

由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素，造成信号沿链路传输损失的能量，称为衰减。衰减是针对“基本回路”/“通道回路”信号损失程度的量度。最坏线对的衰减应小于“基本回路”/“通道回路”允许的最大衰减值。

4)　近端串音(NEXT)衰减

电磁波从一个传输回路(主串回路)串入另一个传输回路(被串回路)的现象称为串音，能量从主串回路串入回路时的衰减称为串音衰减。在 UTP 布线系统中，近端串音为主要的影响因素。布线系统都应通过 NEXT 衰减的测试，而且 NEXT 衰减的测试必须从两个方向进行，也就是双向测试。

5)　回波损耗

回波损耗(RL)是电缆传输系统的一个重要参数。该参数定义为开始输入给信号传输系统的信号与信号源接收到的反射信号的功率之比。不良连接器、操作不当或不正确的线缆拖拉和安装方式都会使线缆产生变形，从而引起回波损耗问题的发生。

2. 光缆布线系统的测试元素及标准

(1)　波长窗口参数。综合布线系统光纤波长窗口的各项参数，应符合表 1-2 的规定。

表 1-2　光纤波长串口参数

光纤模式	波长下限/nm	波长上限/nm	基准试验波长/nm	谱线最大宽度/nm
多模	790	910	850	50
多模	1285	1330	1300	150
单模	1288	1339	1310	10
单模	1525	1575	1550	10

(2)　光缆布线链路的最大衰减限值。综合布线系统的光纤布线链路的衰减限值，应符合表 1-3 的规定。

表 1-3　光纤布线链路的最大衰减限值

应用类别	链路长度/m	多模衰减值/dB		单模衰减值/dB	
		850/nm	1300/nm	1310/nm	1550/nm
水平子系统	100	2.5	2.2	2.2	2.2
垂直子系统	500	3.9	2.6	2.7	2.7
建筑群子系统	1500	7.4	3.6	3.6	3.6

(3) 光回波损耗限值。综合布线系统光纤布线链路任一接口的光回波损耗限值，应符合表 1-4 的规定。

表 1-4　最小的光回波损耗限值

光纤模式、标称波长/nm	最小的光回波损耗限值/dB
多模 850	20
多模 1300	20
单模 1310	26
单模 1550	26

3. 测试环境

(1) 测试条件。综合布线最小模式带宽测试现场应无产生严重电火花的电焊、电钻和产生强磁干扰的设备作业，被测综合布线系统必须是无源网络、无源通信设备。

(2) 测试温度。综合布线测试现场温度在 20～30℃之间，湿度宜在 30%～80%之间，由于衰减指标的测试受测试环境温度影响较大，当测试环境温度超出上述范围时，需要按照有关规定对测试标准和测试数据进行修正。

(3) 测试仪表。按时域原理设计的测试仪均可用于综合布线现场测试，但测试仪的测量扫描步长要满足近端串扰指标测量精度的基本保证，能够在 0～250MHz 频率范围内提供各测试参数的标称值和阈值曲线，每测试一条链路时间不应大于 25s，且每条链路应具有一定的故障定位诊断能力。具有自动、连续、单项选择测试的功能。

4. 测试流程

在开始测试之前，应该认真了解布线系统的特点、用途，信息点的分布情况，确定测试标准。在选定测试仪后按下述程序进行。

(1) 测试仪测试前自检，确认仪表是正常的。

(2) 选择测试方式。

(3) 选择设置线缆类型及测试标准。

(4) 核准 NVP 值。核准 NVP 时使用缆长不短于 15m。

(5) 设置测试环境湿度。

(6) 根据要求选择【自动测试】或【单项测试】命令。

(7) 测试后存储数据并打印。

(8) 发生问题时修复后复测。

(9) 测试中出现“失败”后查找故障。

1.5.2　典型例题分析

例 1　阅读以下说明，回答问题。

【说明】

某公司 A 楼高 40 层，每层高 3.3m，同一楼层内任意两个房间最远传输距离不超过 90m，A 楼和 B 楼之间距离为 500m，需在整个大楼进行综合布线，其结构如图 1-23 所示。

为满足公司业务发展的需要，要求为楼内客户机提供数据速率为 100Mb/s 的数据、图像及语音传输服务。

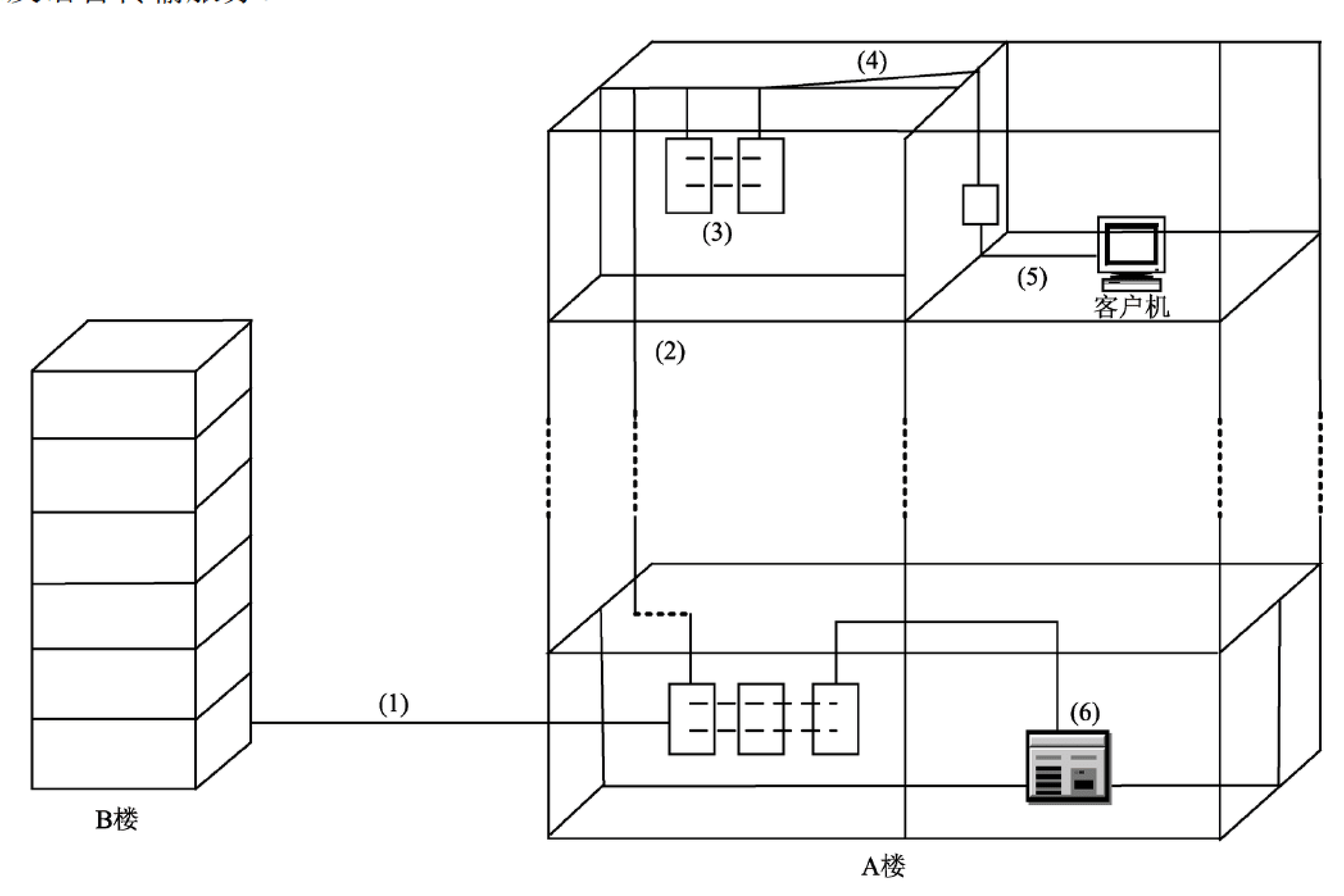


图 1-23　综合布线系统的构成

【问题 1】综合布线系统由 6 个子系统组成，填写出图 1-23 中(1)～(6)处空缺子系统的名称。

【问题 2】考虑性能与价格的因素，图 1-23 中(1)、(2)和(4)中各应采用什么传输介质？

【问题 3】为满足公司的要求，通常选用什么类型的信息插座？

【问题 4】制作交叉双绞线(一端按 EIA/TIA 568A 线序，另一端按 EIA/FFIA 568B 线序)时，其中一端的线序如图 1-24(a)所示，另一端的线序如图 1-24(b)所示，填写图 1-24(b)中(1)～(8)处空缺的颜色名称。

分析：结构化布线可分为 6 个子系统：工作区子系统、水平布线子系统、管理子系统、干线子系统、设备间子系统、建筑群子系统。

随着信息时代的快速发展，数据传递和语音传送并驾齐驱，多媒体技术迅速崛起，如仍采用传统布线，在技术上太落后。综合布线系统采用双绞线与光纤混合的布置方式是比

较科学和经济的方式。

综合布线中采用标准信息插座，型号为 RJ-45，采用 8 芯连线，全部按标准制造，符合 ISDN 标准。在 RJ-45 插座内不仅可以插入数据通信通用的 RJ-45 接头，也可以插入电话机专用 RJ-12 插头。

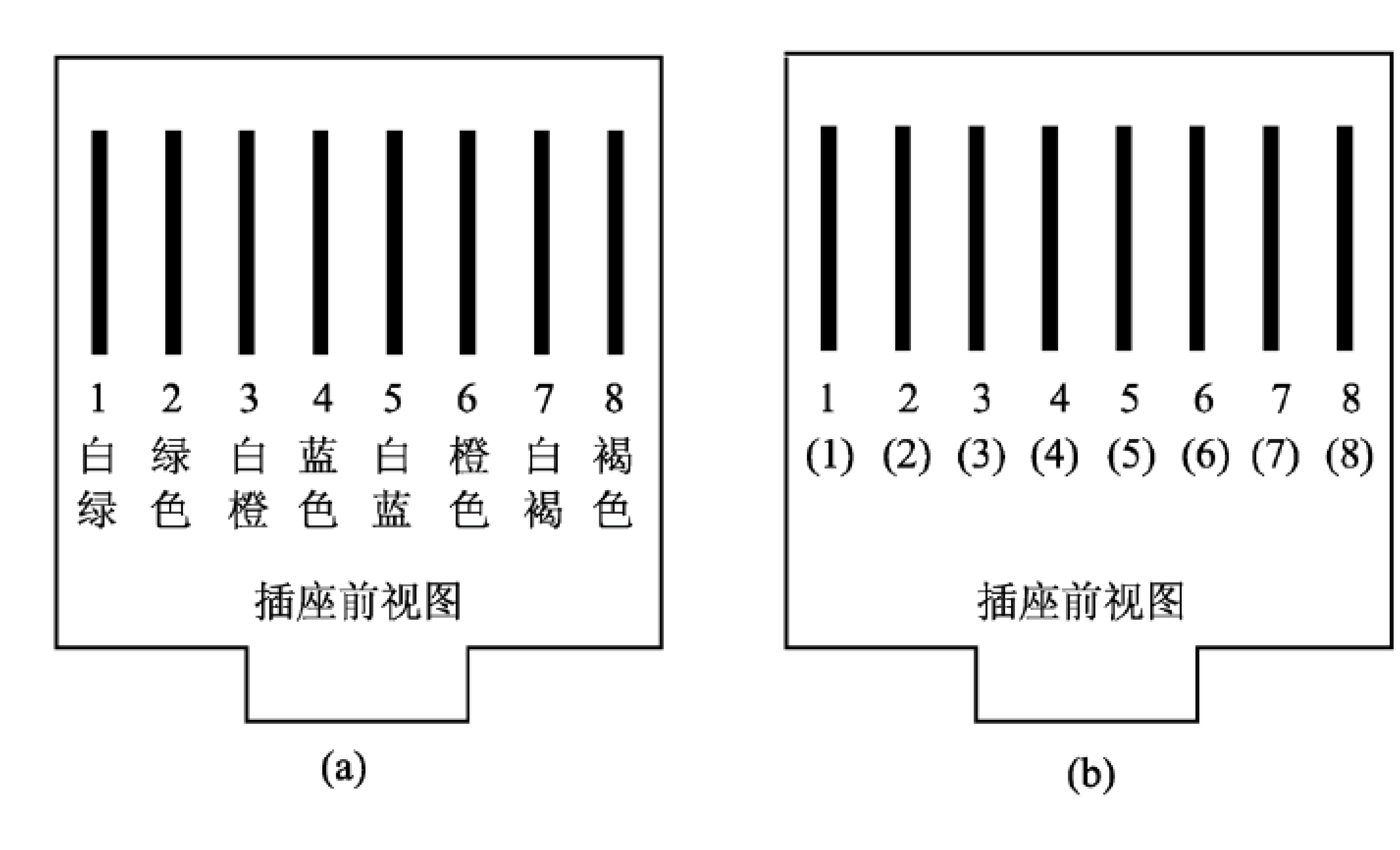


图 1-24　EIA/TIA RJ-45 接口线序

双绞线与交叉线的制作遵循 EIA/TIA568 标准。

答案：

【问题 1】

(1)　建筑群子系统(或户外子系统)

(2)　干线子系统(或垂直子系统)

(3)　管理子系统(或布线、跳线子系统)

(4)　配线子系统(或水平子系统)

(5)　工作区子系统(或用户端子系统)

(6)　设备间子系统(或机布线、跳线子系统)

【问题 2】

(1)　多模光纤

(2)　多模光纤

(3)　5 类双绞线(或超 5 类双绞线)

【问题 3】

RJ-45 插座(或信息模块式超 5 类信息插座、多媒体信息模块式超 5 类信息插座)

【问题 4】

(1)白橙　(2)橙色　(3)白绿　(4)蓝色

(5)白蓝　(6)绿色　(7)白褐　(8)褐色

1.5.3　同步练习

1．什么是综合布线？综合布线的特点是什么？综合布线系统由哪几个子系统构成？

2．在综合布线中，对双绞线进行测试，主要测试哪些元素？

3．在综合布线中，对光纤进行测试，主要测试哪些元素？

1.5.4　同步练习参考答案

1．综合布线系统(PDS)是专为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。

与传统布线系统比较，综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性的特点。

综合布线系统由 6 个子系统组成，即水平子系统、垂直子系统、工作区子系统、管理子系统、设备间子系统及建筑群子系统。

2．连接图、线缆长度、衰减、近端串音衰减、回波损耗。

3．波长窗口、衰减、回波损耗。

1.6　IP 地址及其规划

1.6.1　考点辅导

1.6.1.1　IP 地址基础

Internet 是由不同物理网络互联而成的，不同网络之间实现计算机的相互通信必须有相应的地址标识，这个地址标识称为 IP 地址。图 1-25 所示为 IP 地址的组成与表示。

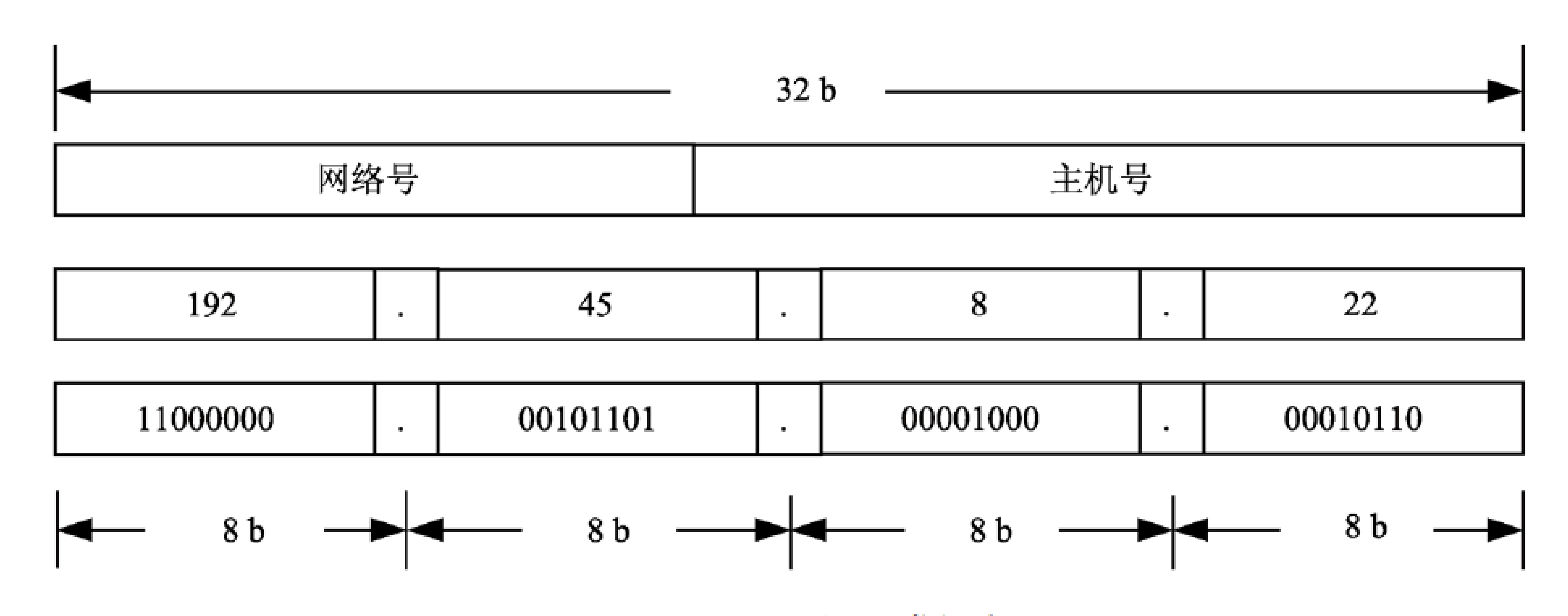


图 1-25　IP 地址的组成与表示

1．IP 地址的组成

一个 IP 地址由网络号和主机号两部分组成。同一个物理网络上的所有主机都用同一个网络号，网络上的每个主机(包括网络上的工作站、服务器和路由器等)都有一个主机号与其对应。据此把 IP 地址划分为两个部分：一部分用以标明具体的网络段，即网络号(net-id)；另一部分用以标明具体的节点，即主机号(host-id)。

2. IP 地址的表示

一个 IP 地址由 4 个字节共 32 位的数字串组成，这 4 个字节通常用小数点分隔。每个字节可用十进制表示，如 192.45.8.22。IP 地址也可以用二进制和十六进制表示。

3. IP 地址的分类

IP 协议的寻址方式支持 5 种不同的网络类型：A 类、B 类、C 类、D 类和 E 类。其中，A、B、C 类地址是基本的 Internet 地址，是用户使用的地址；D 类地址被称为组播地址(多点播送地址)；而 E 类地址尚未使用，以保留给将来使用。IP 地址的最左边的一个或多个二进制位通常用来指定网络的类型。例如，A 类地址的第一位为“0”，B 类地址的前两位为“10”，C 类地址的前三位为“110”。图 1-26 和表 1-5 说明了 5 种不同网络类型 IP 地址的特征和地址容量。

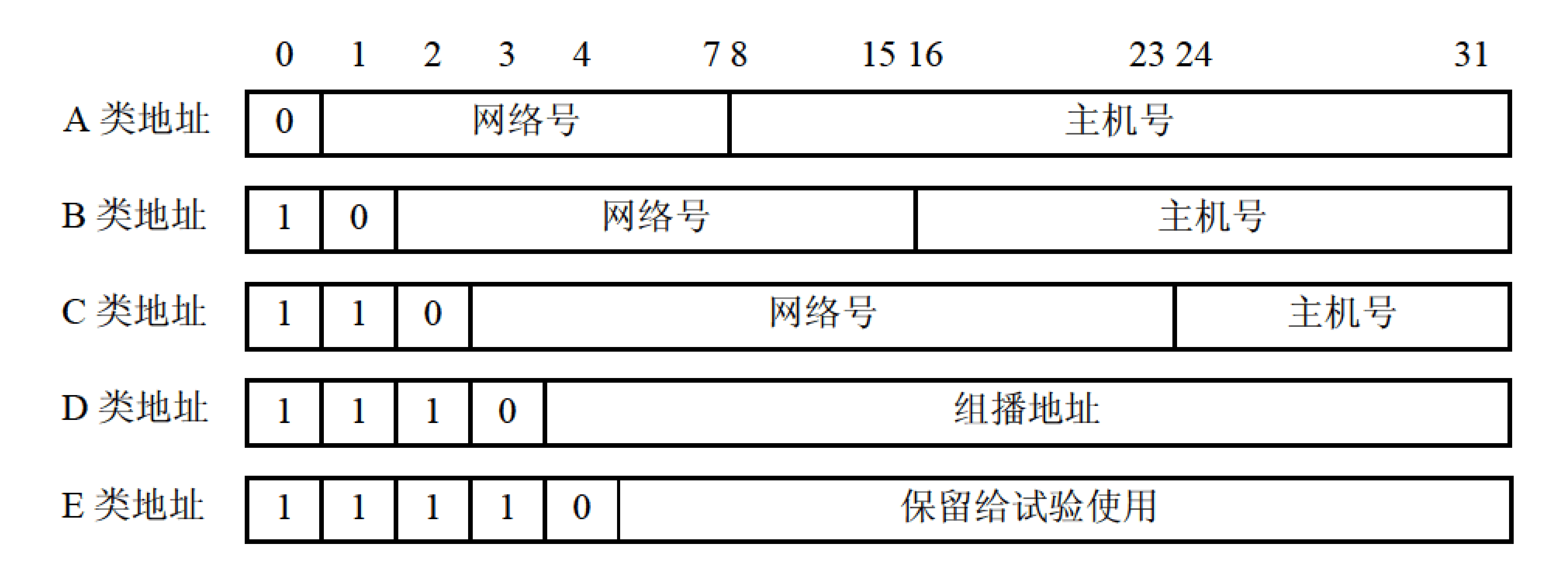


图 1-26 IP 地址的分类

表 1-5 Internet 的 IP 地址空间容量

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位	网络数	二进制主机位	主机数
A 类	0～127	0	8 位	126	24 位	16 777 214
B 类	128～191	10	16 位	16 384	16 位	65 534
C 类	192～223	110	24 位	2 097 152	8 位	254
D 类	224～239	1110	组播地址			
E 类	240～255	11110	保留给试验使用			

A 类：一个 A 类 IP 地址由 1 个字节的网络地址和 3 个字节的主机地址组成，网络地址的最高位必须是“0”(每个字节有 8 位二进制数)。8 位作为网络号，24 位作为主机号，最多可以表示 126 个网络号(0 和 127 用作特殊地址)，每个 A 类地址主机数最多可有 $2^{24}-2$(16 777 214)个。

B 类：一个 B 类 IP 地址由两个字节的网络地址和两个字节的主机地址组成，网络地址的最高两位必须是“10”。16 位作为网络号，16 位作为主机号，最多可以表示 2^{14}(16 384)个网络号，每个 B 类地址主机数最多可有 $2^{16}-2$(65 534)个。

C 类：一个 C 类地址是由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地址的最高三位必须是“110”。24 位作为网络号，8 位作为主机号。共有 2^{21}(2 097 152)个网络

号，每个 C 类地址主机数不超过 2^8-2(254)个。

D 类：用于多点播送。第一个字节以“1110”开始。因此，任何第一个字节大于 223 小于 240 的 IP 地址是组播地址。

E 类：以“11110”开始，是保留给试验使用的地址。

4. IP 地址的特殊形式

IP 地址除了可用于标识一台主机外，还有几种用于表示特殊意义的形式，如表 1-6 所示。

表 1-6　一般不使用的特殊 IP 地址

特殊地址	net-id	host-id	源地址使用	目的地址使用
本网络的本台主机	全 0	全 0	可以	不可以
本网络的某个主机	全 0	host-id	不可以	可以
网络地址	net-id	全 0	可以	可以
直接广播地址	net-id	全 1	不可以	可以
受限广播地址	全 1	全 1	不可以	可以
环回地址	127	任何数	可以	可以

(1) 本网络的本台主机：若一个 IP 地址全由“0”组成，即 0.0.0.0，表示在本网络上的本台主机。当一台主机在运行引导程序但又不知道其 IP 地址时使用该地址。

(2) 本网络的某个主机：网络号各位全为“0”的 IP 地址，表示在这个网络中的特定主机。它用于向同网络中其他主机发送报文。

(3) 网络地址：主机号各位全为“0”的 IP 地址，标识本网络的网络地址。

(4) 直接广播地址(有时简称为广播地址)：主机号各位全为“1”的 IP 地址。它用于将一个分组发送给特定网络上的所有主机，即对全网广播。

(5) 受限广播地址：网络号和主机号都为“1”的 IP 地址(即 255.255.255.255)。它也是对当前网络进行广播，多数是用在当一台主机在运行引导程序时，但又不知道其 IP 地址而需要向服务器获取 IP，这时用该地址作为目的地址发送分组。

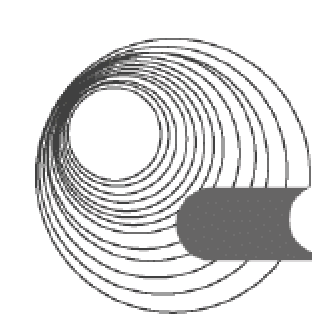
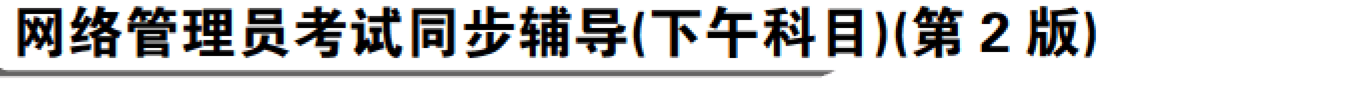
(6) 环回地址(Loopback Address)：A 类网络地址 127.×.×.×是一个保留地址，用于网络软件测试以及本地进程间的通信。

5. 保留 IP 地址

如果一个组织不需要接入到互联网上，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用保留地址。保留地址不需要从互联网管理机构申请，任何组织都可以使用这些地址。这些地址在一个组织内部是惟一的，但从全局来看却不是惟一的。同时互联网的路由器也不转发目标地址为保留地址的数据包。保留地址如表 1-7 所示。

表 1-7　Internet 的保留 IP 地址空间

类　型	网　络　号	网　络　数
A 类	10.0.0.0	1

续表

类　型	网 络 号	网 络 数
B 类	172.16.0.0～172.31.0.0	16
C 类	192.168.0.0～192.168.255.0	256

1.6.1.2　子网的划分

1. 为什么要划分子网

(1) IP 地址空间利用率很低。由于 Internet 的 IP 地址采用两级结构，即网络号和主机号，这样的设计有不够合理的地方。IP 地址中的 A～C 类地址，可供分配的网络号码超过 211 万个，而这些网络上的主机号的总数则超过 37.2 亿个，初看起来，似乎 IP 地址足够全世界来使用(在 20 世纪 70 年代初期设计 IP 地址时就是这样认为的)。其实不然。第一，当初没有预计到计算机会普及得如此之快，各种局域网以及局域网上的主机数目急剧增长。第二，IP 地址在使用时有很大的浪费。例如，某个单位申请到了一个 B 类地址，但该单位只有 1 万台主机。于是，在一个 B 类地址中的其余 55 000 多个主机号就白白地浪费了，因为其他单位的主机无法使用这些号码。

(2) 大型的网络将影响网络性能。从网络吞吐量考虑，将大量主机安装在一个网络上往往会影响网络的性能。当网络上工作的主机数小于一定数值时，网络的吞吐量和网络上工作的主机数大约成正比。但是当网络上工作的主机数超过一定数量时，拥塞就可能产生，这就导致网络的吞吐量增加，速度变慢，网络性能甚至会随着主机数的增加而下降。

(3) IP 地址的两级结构不够灵活。有时情况紧急，一个单位需要在新的地点马上开通一个新网络。但是在申请到一个新的 IP 地址之前，新增加的网络不可能连接到互联网上工作。我们希望有一种方法，使本单位能随时灵活地增加本单位的网络，而不必事先到互联网管理机构去申请新的网络号。原来的两级 IP 地址结构无法做到这一点。

2. 从两级 IP 地址到三级 IP 地址

为了解决上述问题，在 IP 地址中又增加了一个“子网号字段”，使原来两级的 IP 地址变成为三级的 IP 地址，这样就能够较好地解决上述问题，并且使用起来也很灵活。划分子网的基本思路如下。

(1) 一个拥有许多物理网络的单位，可将其物理网络划分为若干个子网(Subnet)。划分子网纯属一个单位内部的事情，本单位以外的网络看不见这个网络由多少子网组成，对外仍表现为一个没有划分子网的网络。

(2) 划分子网的方法是从 IP 地址的主机号借用若干位作为子网号 subnet-id，而主机号 host-id 也就相应地减少了若干位。于是，两级的 IP 地址在本单位内部就变为三级 IP 地址：网络号 net-id、子网号 subnet-id 和主机号 host-id，如图 1-27 所示。

(3) 凡是从其他网络发送给本单位某个主机的 IP 数据报，仍然是根据 IP 数据报的目的网络号 net-id 找到连接在本单位网络上的路由器。但此路由器在收到 IP 数据报后，再按目的网络号 net-id 和子网号 subnet-id 找到目的子网，并将 IP 数据报交付给目的主机。

下面用一个例子来说明划分子网的概念。一个单位拥有一个 B 类 IP 地址，网络地址是 141.14.0.0(net-id 是 141.14)。凡目的地址为 141.14.×.×的数据报都被送到这个网络上的路

由器 R1。

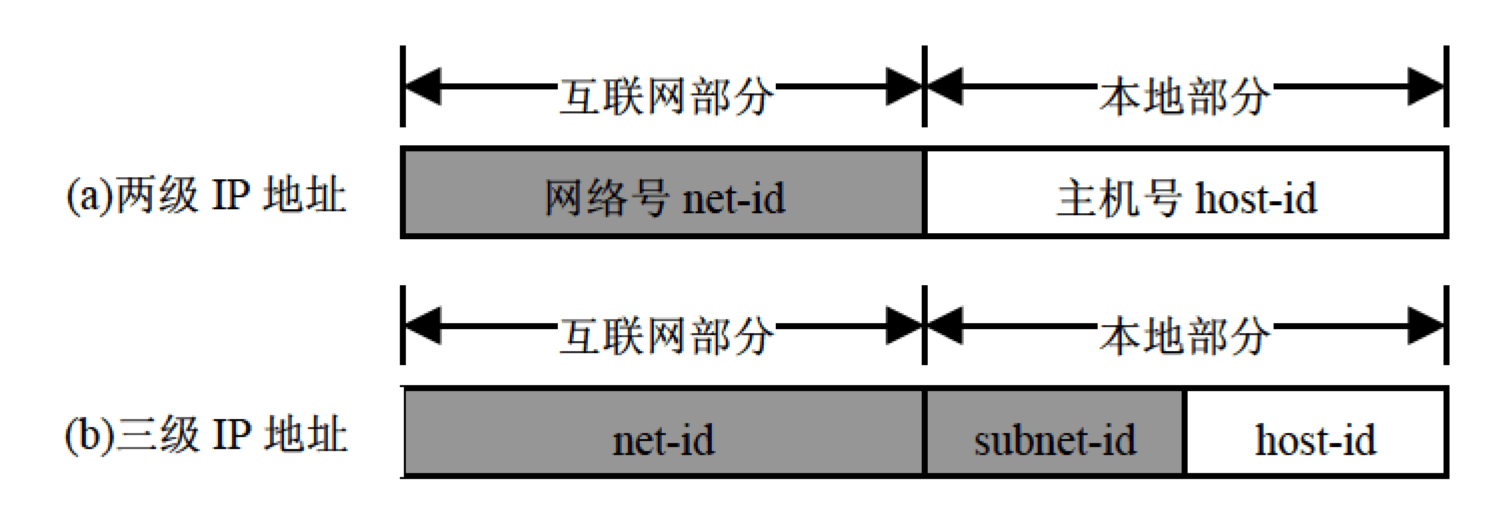


图 1-27　从两级 IP 地址到三级 IP 地址(一)

现将图 1-28 的网络划分为三个子网，如图 1-29 所示。这里假设子网号 subnet-id 占 8 位，因此在增加子网号后，主机号 host-id 就只有 8 位。所划分的三个子网分别是：141.14.2.0、141.14.7.0 和 141.14.99.0。在划分子网后，整个网络对外仍表现为一个网络，其网络地址仍然是 141.14.0.0。但路由器 R1 收到数据报后，再根据数据报的目的地址将其转发到相应的子网。

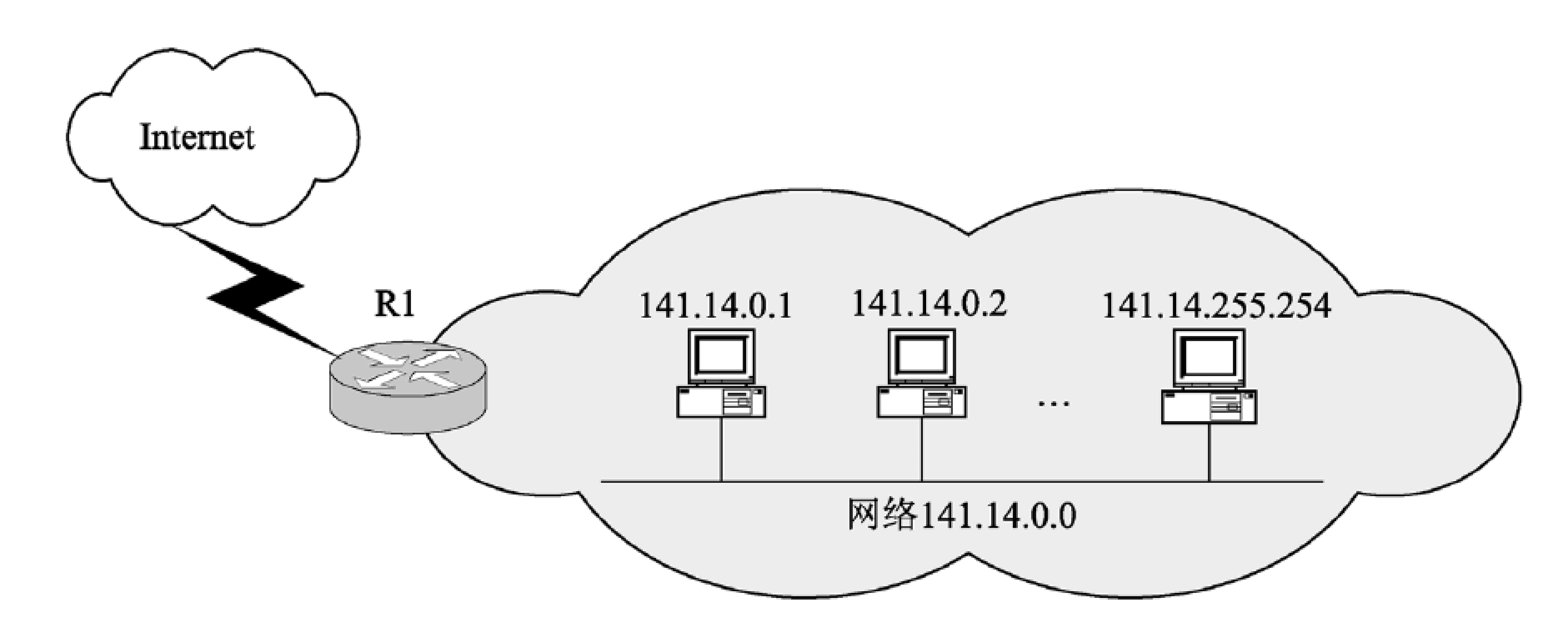


图 1-28　从两级 IP 地址到三级 IP 地址(二)

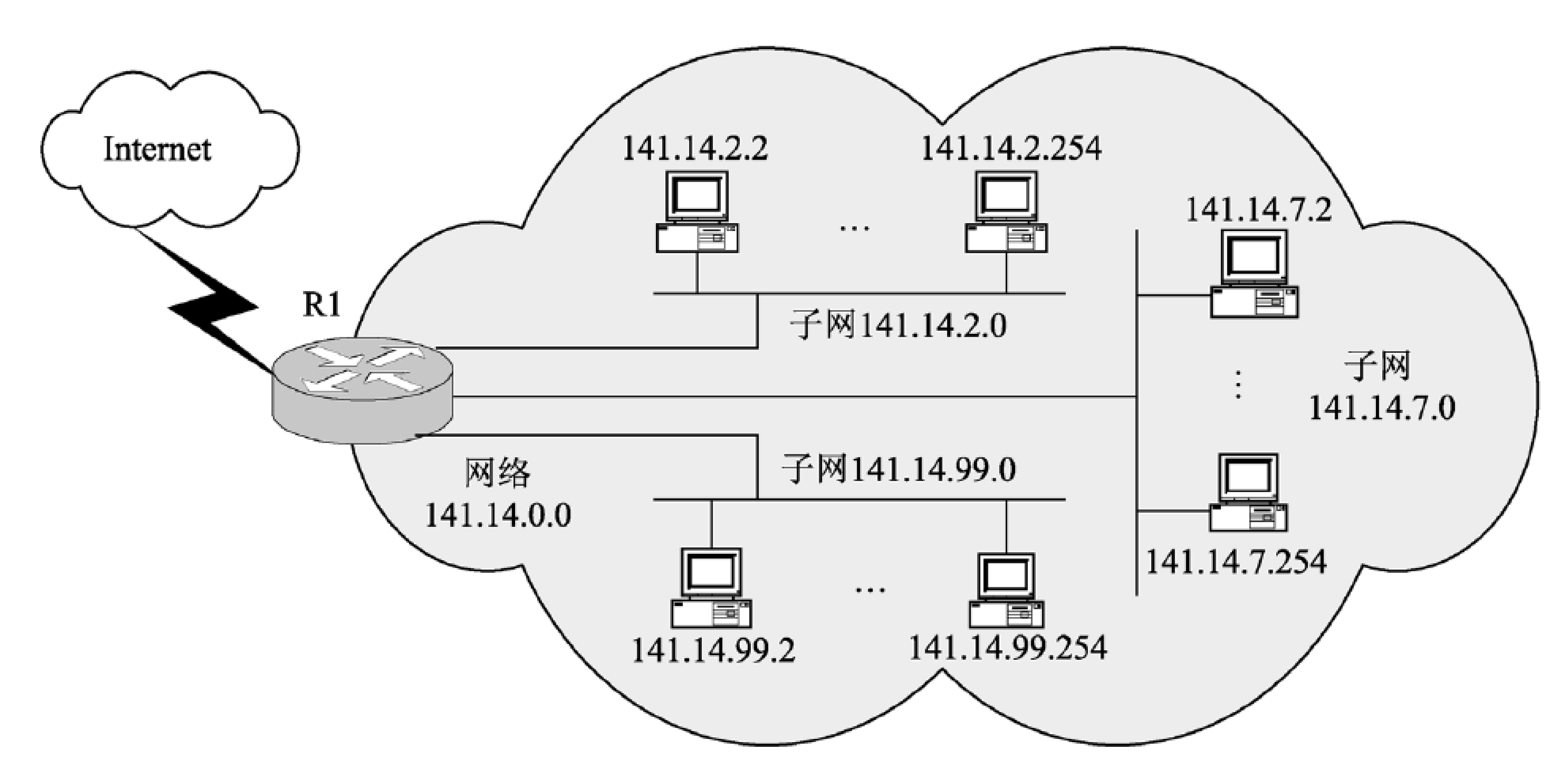


图 1-29　从两级 IP 地址到三级 IP 地址(三)

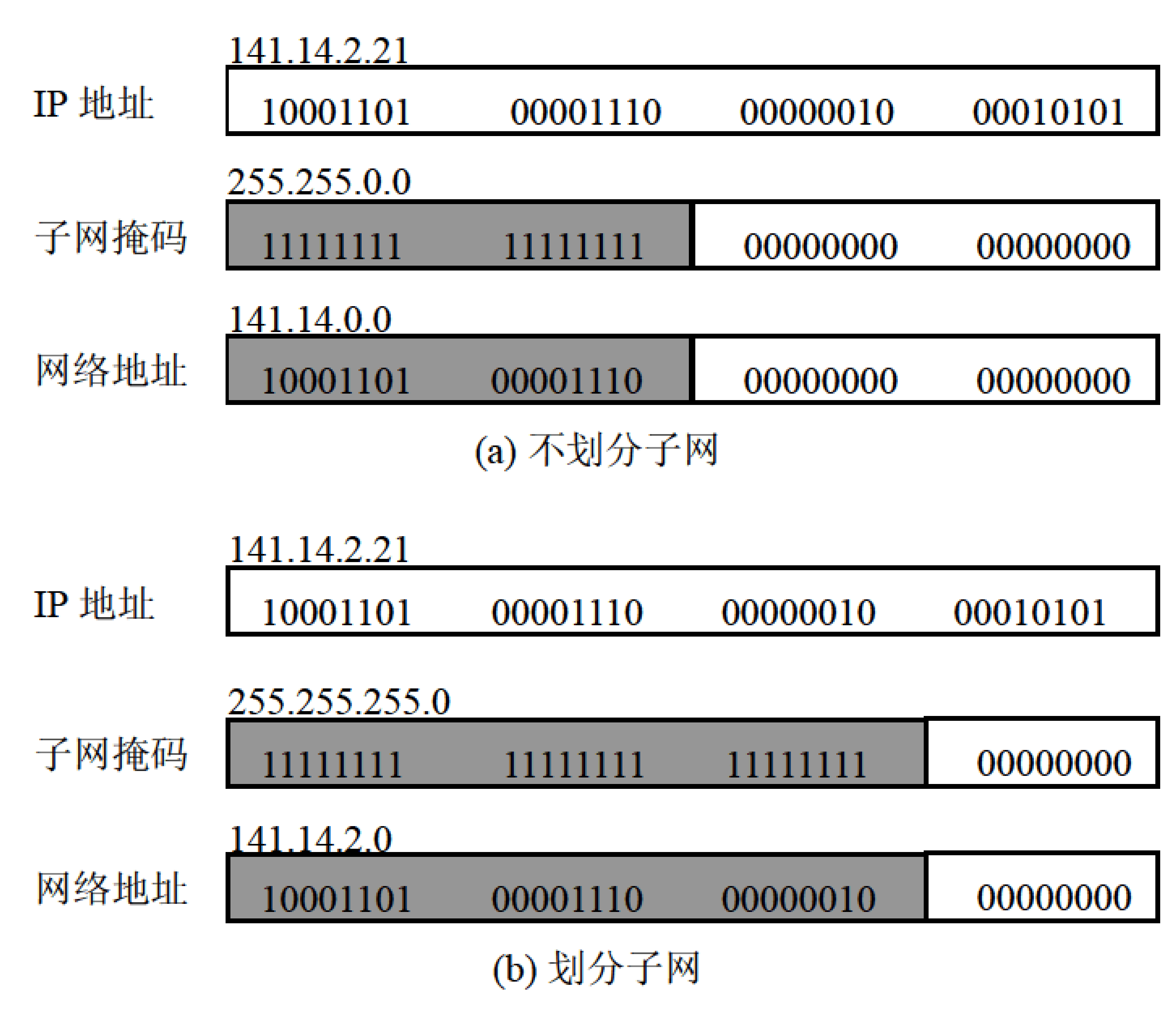
3. 子网掩码

虽然上面已经把一个网络划分为若干个子网，但路由器 R1 必须知道数据报中目的 IP

地址的网络号 net-id、子网号 subnet-id 和主机号 host-id 各是多少位，这就需要通过子网掩码(Subnet mask)来实现。

子网掩码和 IP 地址一样，也是 32 位长，由一串 1 和跟随的一串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号 net-id 和子网号 subnet-id，而子网掩码中的 0 对应于 IP 地址中的主机号 host-id。要得到网络或子网地址，只需将 IP 地址和子网掩码进行按位“与”(AND)运算即可。图 1-23 说明了子网掩码的工作方式。

图 1-30(a)表示在未划分子网情况下，网络地址是 IP 地址与它默认的子网掩码(255.255.0.0)按位“与”运算的结果，即将主机号 host-id 置为 0 的 IP 地址。图 1-30(b)表示在划分子网情况下，当主机号借用 8 位作为子网号 subnet-id，子网掩码中“1”的个数相应地增加 8，即(255.255.255.0)。这时将子网掩码和 IP 地址按位“与”运算就得到了子网地址。这里要注意是：网络地址(在划分子网时常称为子网地址)并不仅仅是一个子网号 subnet-id，而是将主机号 host-id 置为 0 的 IP 地址。可以看出，子网掩码不能单独存在，它必须结合 IP 地址一起使用。



(a) 不划分子网

(b) 划分子网

图 1-30 进行按位“与”(AND)运算可得到网络地址

与 IP 地址相同，子网掩码通常也使用点分十进制表示法表示，例如，255.255.255.0、255.255.255.240 等。有时为了表示方便，通常在 IP 地址后加一个“/网络号和子网号位数”。例如，210.45.12.58/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位，主机号占用 32−28=4 位，如果用点分十进制表示法表示，则子网掩码是 255.255.255.240 (11111111.11111111.11111111.11110000)。

使用子网掩码的好处是：不管网络是否划分子网，也不管 IP 地址中的网络号 net-id 和子网号 subnet-id 是多少位，只要将子网掩码和 IP 地址进行按位“与”运算，就可立即得出网络地址来。这样在路由器处理到来的 IP 分组时就可采用同样的算法。

如果一个网络不划分子网，那么该网络的子网掩码就使用默认子网掩码。默认子网掩

码中值为 1 的位与 IP 地址的网络号 net-id 所占位正好相对应。因此默认子网掩码和不划分子网的 IP 地址按位“与”(AND)运算，就得出该 IP 地址的网络地址来，这样做就可以不用查找该地址的分类位就能知道这是哪一类的 IP 地址。显然，A 类、B 类和 C 类网络默认子网掩码分别是 255.0.0.0(/8)、255.255.0.0(/16)、255.255.255.0(/24)，如图 1-31 所示。

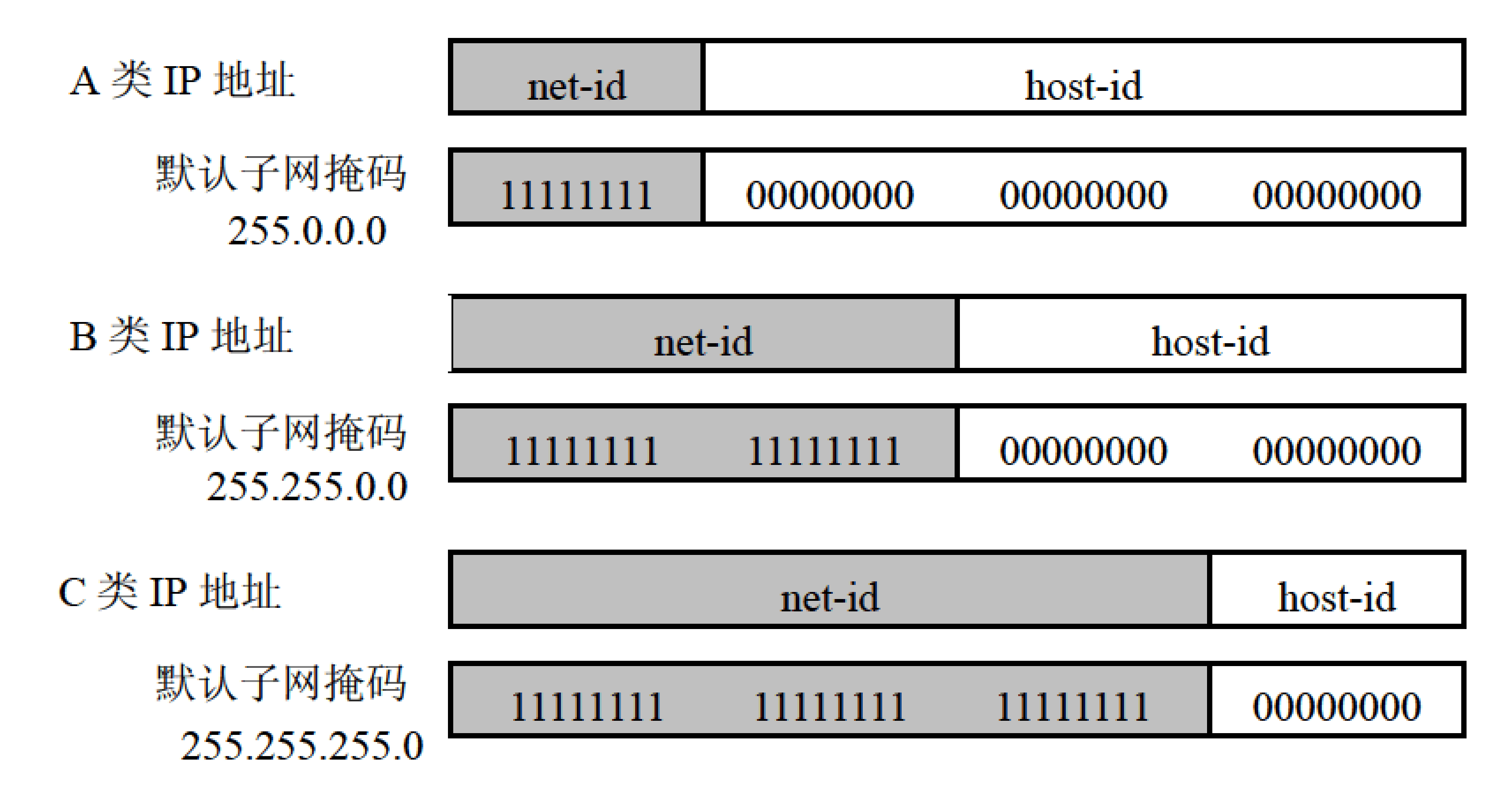


图 1-31　A 类、B 类和 C 类 IP 地址的默认子网掩码

4. 划分子网示例

1) B 类地址的子网规划示例

B 类地址由两个字节的网络号 net-id 和两个字节的主机号 host-id 组成。一个得到 B 类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达 65 534(2^{16}−2)个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围。表 1-8 说明了一个 B 类地址可以有多少种子网划分的方法。在采用固定长度子网时，划分的所有子网的子网掩码都是相同的。

表 1-8　B 类地址的子网划分选择(使用固定长度子网)

子网位数	子网掩码	子 网 数	主 机 数
2	255.255.192.0	2	16 382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14


续表

子网位数	子网掩码	子 网 数	主 机 数
13	255.255.255.248	8190	6
14	255.255.255.252	16 382	2

例如，一个具有 B 类地址的组织的网络号为 X.Y.0.0(128≤X≤191)，需要至少 12 个子网，试找出子网掩码和每个子网的配置。因为需要至少 12 个子网，因此至少需要向主机号 host-id 借 4 位(2^3−2≤12≤2^4−2)来构造子网，网络号 net-id 和子网号 subnet-id 共 12 位(8+4=12)，所以子网掩码为 11111111.11111111.11110000.00000000，即 255.255.240.0。每个子网有 4096(2^{12}=4096)个地址，其中第一个地址用来定义子网(子网地址)，而最后一个地址用于子网内广播(广播地址)，这就表明连接到每一个子网上的计算机数最多是 4094。表 1-9 是每一个子网的地址范围。

表 1-9　B 类地址的子网划分示例(使用固定长度子网)

子　网	子网地址	地址范围	广播地址	说　明
第 0 个子网	X.Y.0.0	X.Y.0.1～X.Y.15.254	X.Y.15.255	保留，不可用
第 1 个子网	X.Y.16.0	X.Y.16.1～X.Y.31.254	X.Y.31.255	可用
第 2 个子网	X.Y.32.0	X.Y.32.0～X.Y.47.254	X.Y.47.255	可用
⋮	⋮	⋮	⋮	可用
第 14 个子网	X.Y.224.0	X.Y.224.0～X.Y.239.254	X.Y.239.255	可用
第 15 个子网	X.Y.240.0	X.Y.240.1～X.Y.255.254	X.Y.255.255	保留，不可用

注意：根据 RFC 950 的规定，进行子网划分时，对于子网号 subnet-id 为全 0 和全 1 的子网不允许使用，因此表 1-9 中，第 0 个子网和第 15 个子网是不可用的。但随着无分类域间路由选择 CIDR 的广泛使用，现在全 0 和全 1 的子网也可以使用，但一定要谨慎使用，要弄清所使用的路由器是否支持全 0 和全 1 的子网。

2)　C 类地址的子网规划示例

C 类地址由三个字节的网络号 net-id 和一个字节的主机号 host-id 组成。一个得到 C 类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达 254(2^8−2)个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围。表 1-10 说明了一个 C 类地址可以有多少种子网划分的方法(在采用固定长度子网时，划分的所有子网的子网掩码都是相同的)。

表 1-10　C 类地址的子网划分选择(使用固定长度子网)

子网位数	子网掩码	子 网 数	主 机 数
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14

续表

子网位数	子网掩码	子 网 数	主 机 数
5	255.255.255.248	30	6
6	255.255.255.252	62	2

例如，一个具有 C 类地址的组织的网络号为 X.Y.Z.0(192≤X≤223)，需要至少 5 个子网，试找出子网掩码和每个子网的配置。因为需要至少 5 个子网，划分时至少要 7 个子网，5 个是可用的，两个保留为特殊地址不可用，因此至少需要向主机号 host-id 借 3 位($2^2-2\leqslant5\leqslant2^3-2$)来构造子网，网络号 net-id 和子网号 subnet-id 共 27(24+3)位，所以子网掩码为 11111111.11111111.11111111.11100000，即 255.255.255.224。每个子网有 32 个($2^5=32$)地址，其中第一个地址用来定义子网(子网地址)，而最后一个地址用于子网内广播(广播地址)，这就表明连接到每一个子网上的计算机数最多是 30。表 1-11 是每一个子网的地址范围。

A 类地址的子网规划方法与 B 类、C 类相似，因篇幅所限，这里不作详细介绍。

表 1-11　C 类地址的子网划分实例(使用固定长度子网)

子　网	子网地址	地址范围	广播地址	说　明
第 0 个子网	X.Y.Z.0	X.Y.Z.1～X.Y.Z.30	X.Y.Z.31	保留，不可用
第 1 个子网	X.Y.Z.32	X.Y.Z.33～X.Y.Z.62	X.Y.Z.63	可用
第 2 个子网	X.Y.Z.64	X.Y.Z.65～X.Y.Z.94	X.Y.Z.95	可用
⋮	⋮	⋮	⋮	可用
第 6 个子网	X.Y.Z.192	X.Y.Z.193～X.Y.Z.222	X.Y.Z.223	可用
第 7 个子网	X.Y.Z.224	X.Y.Z.225～X.Y.Z.254	X.Y.Z.255	保留，不可用

5. 可变长子网掩码(VLSM)

互联网允许一个地点使用变长子网划分。下面举例说明什么时候有这种需要。例如，一个具有 C 类地址的地点需要划分为 5 个子网，其连接的主机数分别为 60、60、60、30 和 30。这个地点不能使用给子网分配两个位的掩码，因为这样将只有 4 个可连接 62(256/4−2=62)台主机的子网。在这个地点使用给子网分配三个位的掩码也不行，因为这样将有 8 个可连接 30(256/8−2=30)台主机的子网(应注意，这里放松了对特殊地址的要求，即子网号为全 0 和全 1 可用)。

解决这个问题的一种方法是使用变长子网划分。在这种配置中，路由器使用两个不同的掩码。它先使用具有 26 个 1 的掩码(11111111.11111111.11111111.11000000 或 255.255.255.192)，将网络划分为 4 个子网。然后再对其中的一个子网使用具有 27 个 1 的掩码(11111111.11111111.11111111.11100000 或 255.255.255.224)，将其划分为两个更小的子网(见图 1-32)。

1.6.1.3　超网和无分类编址

虽然 A 类和 B 类地址几乎用完了，但 C 类地址目前还能申请到。然而 C 类地址空间只能容纳最多 254 台主机，这可能无法满足一个组织的需要，甚至一个中等规模的组织也会需要更多的地址。

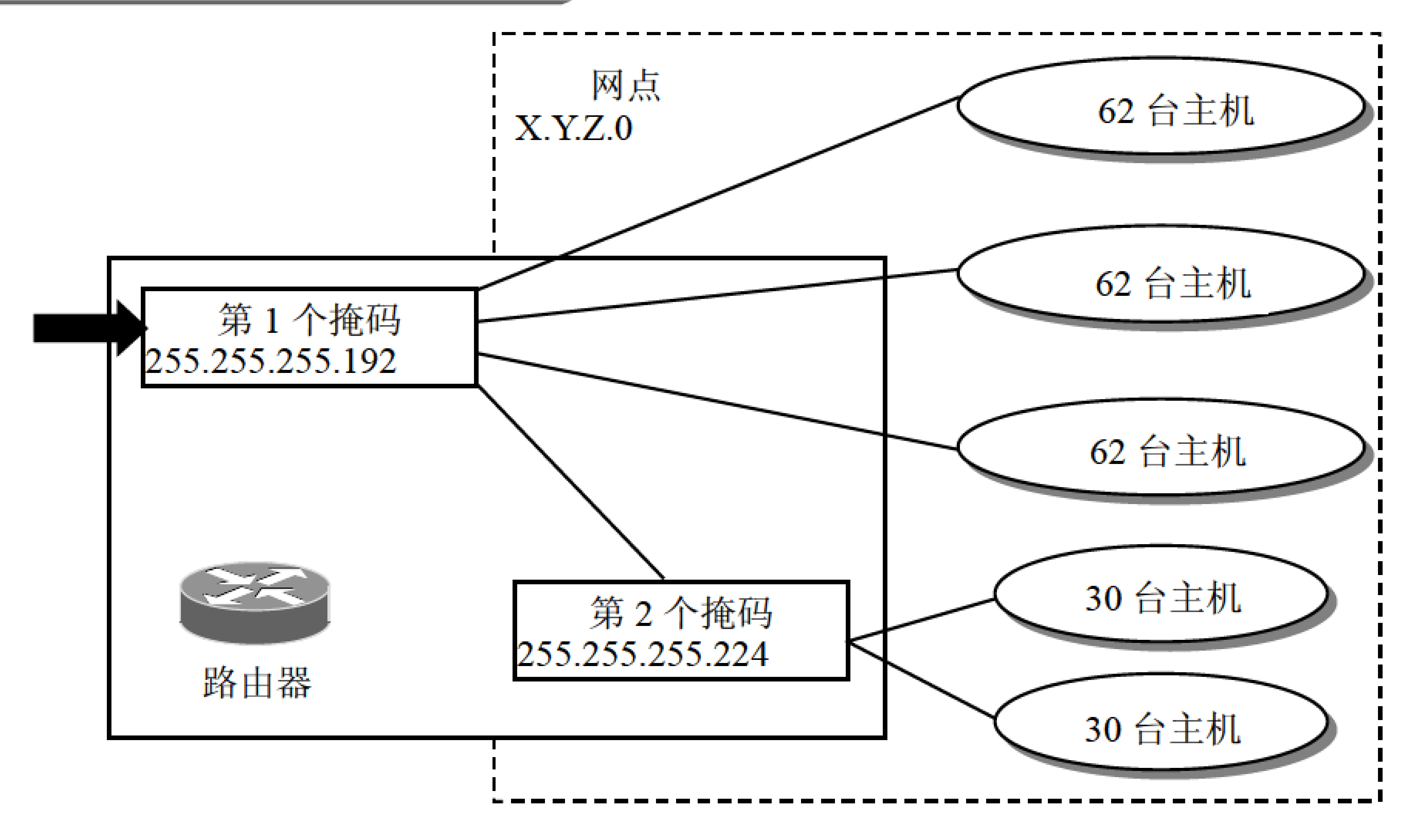


图 1-32 可变长子网划分

一种解决问题的方法是构成超网(Supernet)。为此，一个组织可申请一块而不是只申请一个 C 类地址。例如，一个需要 1000 个地址的组织可申请 4 个 C 类地址。这个组织就可以在一个超网中、在 4 个网络中或在超过 4 个子网中使用这些地址。在图 1-33 中，4 个 C 类地址合并为一个超网。

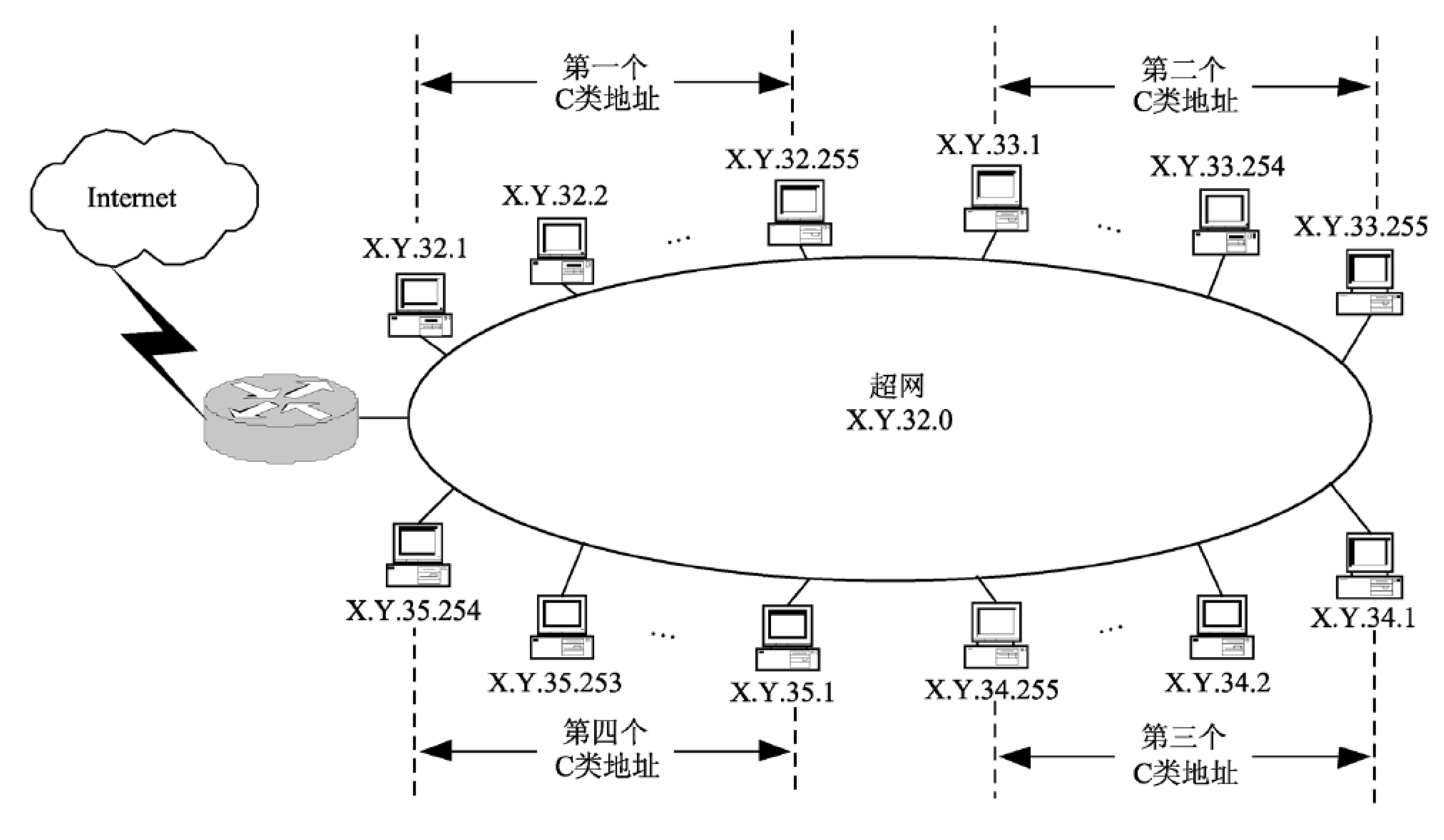


图 1-33 超网

若要给超网掩码指派一块 C 类网络地址，只要地址数是 2 的整数次方(2，4，8，16，…)即可。C 类地址的默认掩码是 255.255.255.0，即 24 个 1 后面跟上 8 个 0。如果将其中的某些 1 改变为 0，我们就可得到一组 C 类地址的超网掩码。超网掩码与子网掩码中的一些做法相反。在子网掩码中，我们将默认掩码中的 host-id 部分的某些 0 改变为 1。在超网掩码中，我们将 net-id 部分中的某些 1 改变为 0。要注意到，在超网掩码中全 1 的位置定义了最低地址。例如图 1-34 所示的超网掩码，开始地址可以是 X.Y.32.0，但不能是 X.Y.33.0。将最低

地址与超网掩码组合起来就能惟一地定义属于一个超网的地址范围，另一个定义地址范围的方法是使用最低地址和在此范围内的地址数来定义。

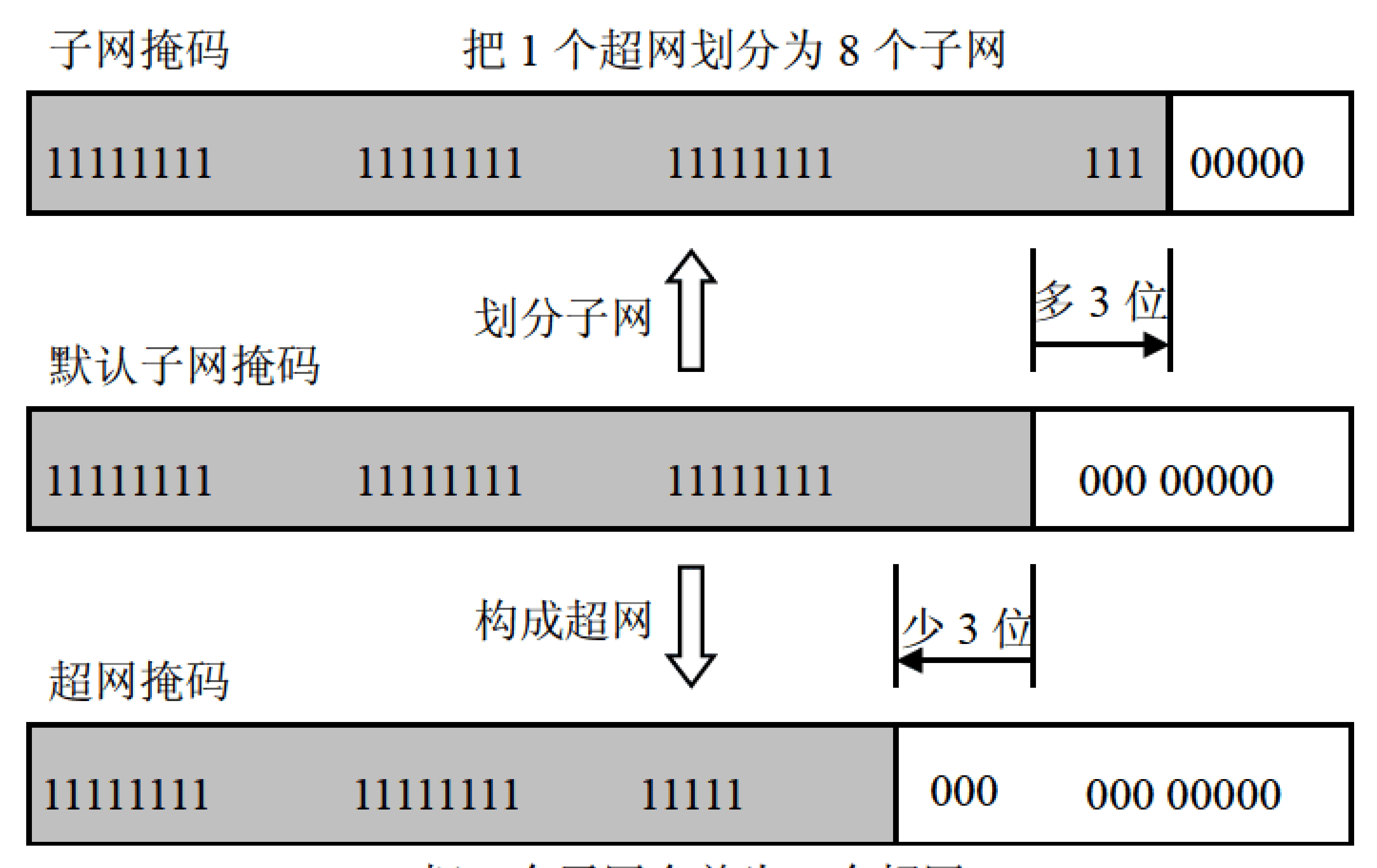


图 1-34　超网掩码

例如，用超网掩码 255.255.252.0 可以将 4 个 C 类地址合并为一个超网。如果我们选择的第一个地址是 X.Y.32.0，则其他三个地址就是 X.Y.33.0、X.Y.34.0 和 X.Y.35.0。当路由器收到一个分组时，就将超网掩码与目的地址作按位“与”(AND)运算，并将结果与最低地址相比较。若结果与最低地址一致，则该分组就属于这个超网。

假定一个分组到达目的地址 X.Y.33.4。在同掩码 255.255.252.0 作按位“与”(AND)运算后，结果为 X.Y.32.0，它与最低地址一致，因此该分组属于这个超网。

现在假定目的地址为 X.Y.39.12 的分组到达。在同掩码 255.255.252.0 作按位“与”(AND)运算后，结果为 X.Y.36.0，它与最低地址不一致，因此该分组不属于这个超网。

在 VLSM 的基础上又进一步研究出无分类编址方法，它的正式名称是无分类域间路由选择(Classless Inter-Domain Routing，CIDR)。CIDR 最主要的特点有两个。

一是 CIDR 消除了传统 A 类、B 类和 C 类地址以及划分子网的概念，从而更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(Network-Prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一个斜线“/”，然后写上网络前缀所占的位数(这个数值对应于三级编址中子网掩码中位 1 的个数)。例如，128.14.146.158/20，表示在这 32 位中，前 20 位表示网络前缀，而后面 12 位为主机号。

二是 CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(地址块中数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示，例如，128.14.32.0/20 表示的地址块共有 2^{12} 个地址，而这个地址的起始地址是 128.14.32.0。

1.6.2　典型例题分析

例1　阅读以下说明，回答问题1至问题6，将解答填入答题纸对应的解答栏内。(2008年11月下午试题二)

【说明】

某公司有人力资源部和销售部两个部门，各有26台主机序需接入Internet。其中销售部同时在线用户数通常小于15。ISP为公司分配的网段为200.101.110.128/26，公司人力资源部采用固定IP地址，销售部采用动态IP地址分配策略，将人力资源部和销售部划归不同的网段，连接方式如图1-35所示。

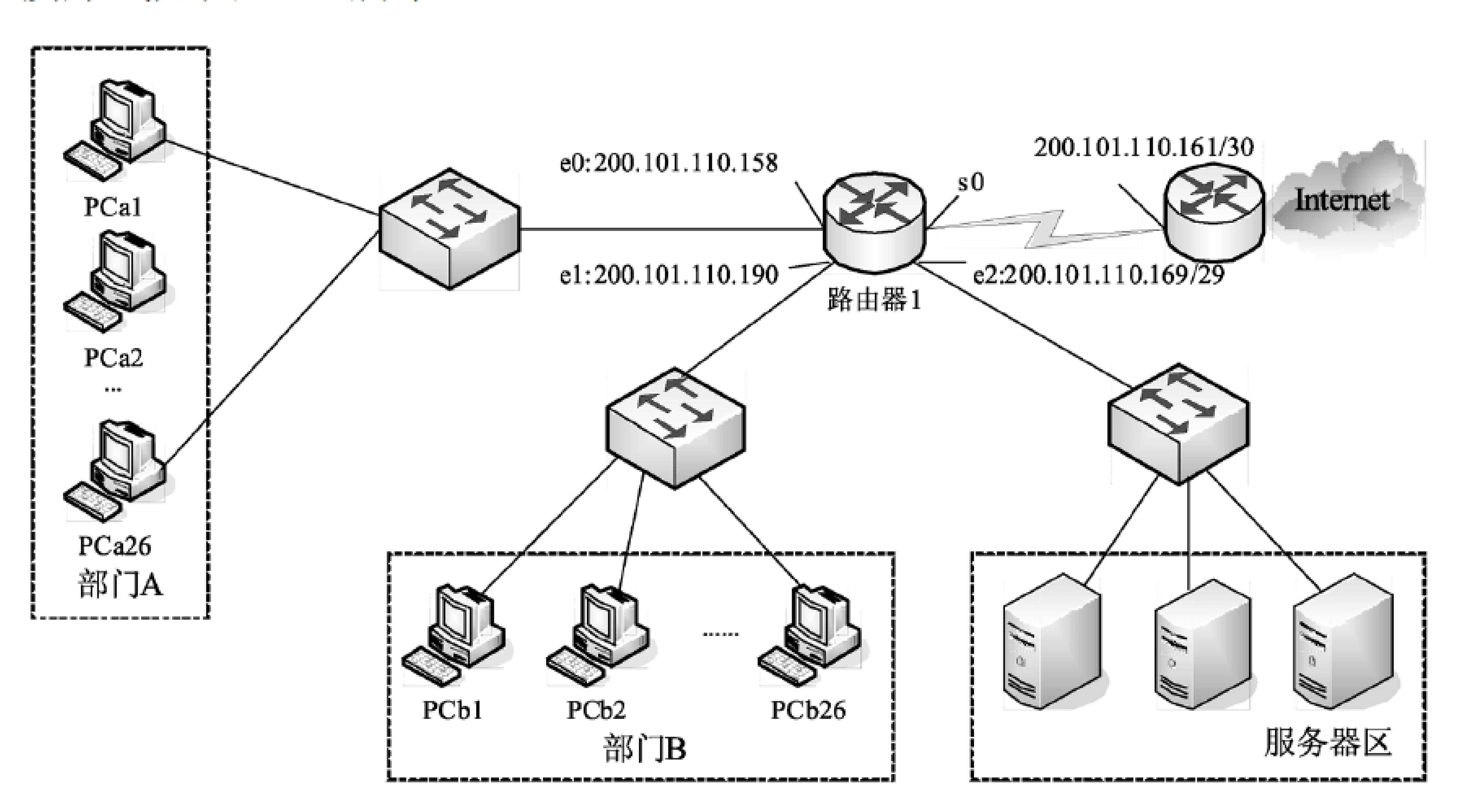


图1-35　人力资源部和销售部连接方式

【问题1】(2分)

如果每台服务器都分配不同的IP地址，服务器区最多可以配置__(1)__台服务器。

【问题2】(2分)

人力资源部是部门A还是部门B？

【问题3】(每空1分，共3分)

为人力资源部的某台PC配置Internet协议属性参数。

IP地址：　　　　　__(2)__

子网掩码：　　　　__(3)__

默认网关：　　　　__(4)__

【问题4】(每空2分，共4分)

为路由器1的s0口配置Internet协议属性参数。

IP地址：　　　　　__(5)__

子网掩码：　　　　__(6)__

【问题5】(2分)

销售部能动态分配的IP地址区间为__(7)__。

【问题 6】(2 分)

若交换机和 PC 之间传输介质采用 5 类 UTP，PC 端采用线序满足 EIA/TIA 568B 标准，则交换机端线序应满足__(8)__。

备选答案：

A. EIA/TIA 568B　　B. EIA/TIA 568A

分析：

【问题 1】

整个服务器区构成一个子网，路由器 e2 口为服务器区的网关，其 IP 地址为 200.101.110.169/29，可知子网掩码对应的前 29 位用于标识子网，剩下的 3 位可用于标识服务器。IP 地址有 2^3=8 个，全 0 和全 1 分别表示子网号和用于广播，路由器 e2 口需要使用 1 个 IP 地址，故可供服务器分配的地址只有 5 个。

【问题 2】

整个公司分配的 IP 地址为 200.101.110.128/26，将这个地址的主机地址部分的最高位依取值 0 或 1 划分成两个子网：200.101.110.128/27 和 200.101.110.160/27，则每个子网可容纳的主机数为 2^5−2=30>26，可以满足要求。每个子网可分配的 IP 地址分别为 200.101.110.129～200.101.110.158，200.101.110.161～200.101.110.190。

由图 1-35 可知，200.101.110.161～200.101.110.190 的 IP 地址范围内有部分被分配给了服务器区和路由器其他端口，因此只有由 200.101.110.158 作为网关的子网才能满足人力资源部这一需求，因此人力资源部是部门 A。

【问题 3】

由问题 2 的分析可知，人力资源部的子网为 200.101.110.158/27，网关为 200.101.110.158，可分配的 IP 地址范围应为 200.101.110.129～200.101.110.157，IP 地址的前 27 位为网络号，因此子网掩码为 255.255.255.224。

【问题 4】

路由器 1 的 s0 口对端的 ISP 路由器端口 IP 地址为 200.101.110.161/30，s0 与其应构成一个子网，可用的 IP 地址范围为 200.101.110.161～200.101.110.162，因此 s0 口的 IP 地址应为 200.101.110.162，子网掩码应为 255.255.255.252。

【问题 5】

除去人力资源部的 IP 地址区间 200.101.110.129～200.101.110.158，200.101.110.161～200.101.110.190 用于路由器、服务器、销售部。其中，服务器区所占的 IP 地址范围为 200.101.110.169～200.101.110.175，路由器还占用了 200.101.110.161～200.101.110.163、200.101.110.190，因此能供销售部动态分配的 IP 地址区间为 200.101.110.164～168 和 200.101.110.176～189。

【问题 6】

交换机和 PC 之间需采用直联方式，交换机端线序应满足 EIA/TIA 568B 标准，故选 A。

答案：

【问题 1】

(1)　5

【问题 2】

部门 A

【问题 3】

(2) 200.101.110.129～200.101.110.157 中任意一个均可

(3) 255.255.255.224

(4) 200.101.110.158

【问题 4】

(5) 200.101.110.162　　　(6) 255.255.255.252

【问题 5】

(7) 200.101.110.176～189 和 200.101.110.164～168

【问题 6】

(8) A

例 2　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2007 年 11 月下午试题一)

【说明】

某公司网络结构如图 1-36 所示。其中网管中心位于 A 楼，B 楼与 A 楼距离约 300m，B 楼的某一层路由器采用 NAT 技术进行网络地址变换，其他层仅标出了楼层交换机。

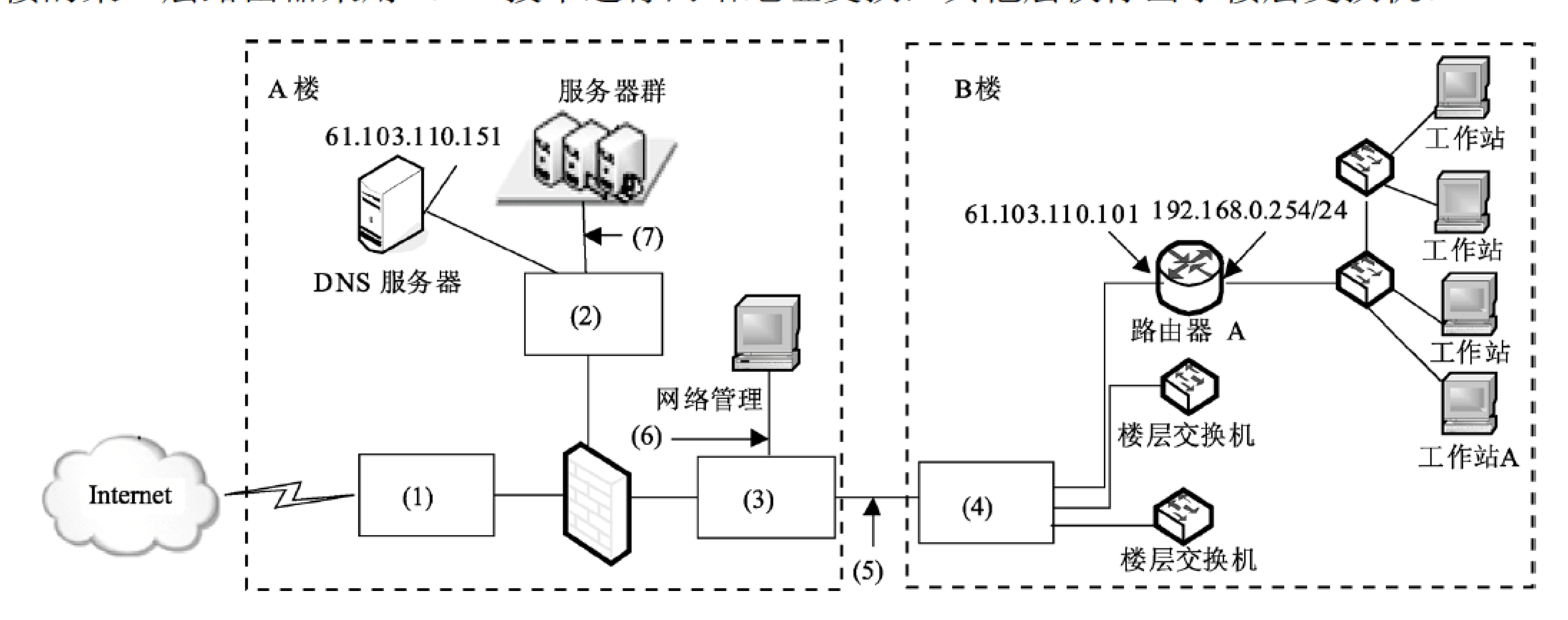


图 1-36　某公司网络拓扑结构

【问题 1】(4 分)

从表 1-12 中为图 1-36 中(1)～(4)处选择合适设备名称(每个设备限选一次)。

表 1-12　网络设备说明表

设备类型	设备名称	数　量
路由器	Router1	1
三层交换机	Switch1	1
二层交换机	Switch2	2

【问题 2】(3 分)

为图 1-36 中(5)～(7)处选择介质，并填写在答题纸的相应位置。

备选介质(每种介质限选一次)：百兆双绞线　千兆双绞线　千兆光纤

【问题 3】(4 分)

表 1-13 是路由器 A 上的地址变换表，将图 1-37 中(8)～(11)处空缺的信息填写在答题纸的相应位置。

表 1-13　路由器 A 的 NAT 变换表

内部 IP/端口号	变换后的端口号
192.168.0.1：1358	34 576
192.168.0.3：1252	65 534



图 1-37　路由器 A

【问题 4】(4 分)

参照图 1-36 的网络结构，为工作站 A 配置 Internet 协议属性参数。

IP 地址：　(12)

子网掩码：　(13)

默认网关：　(14)

首选 DNS 服务器：　(15)

分析：

【问题 1】

考查网络设备的选择。(1)处要为整个网络 Internet 接入时进行路由，故应填入路由器；在剩下的交换机选择中，网络中交换的核心在(3)处，应选三层交换机；(2)、(4)处应选两个二层交换机。

【问题 2】

考查介质的选择。由于 B 楼与 A 楼距离约 300m，故(5)处应选光纤；服务器群与交换机的连接速率要求较网络管理高，故(6)处应选百兆双绞线，(7)处应选千兆双绞线。

【问题 3】

考查路由器上 NAT 变换的理解情况。

NAT 就是在局域网内部网络中使用内部地址，而当内部节点要与外部网络进行通信时，就在网关处将内部地址替换为公用地址，从而在外部公网上正常使用。如果子网中有多个主机要同时通信，那么还要对端口号进行翻译，所以这种技术经常被称为网络地址和端口

翻译。由于变换前源地址和端口号分别为 192.168.0.3 和 1252，查 NAT 表找到对应的端口号为 192.168.0.3 和 65534，从图 1-37 中可以看到映射后的公网 IP 地址为 61.103.110.101，故(8)、(9)应分别填入 61.103.110.101 和 65534；由于变换后目的地址和端口都不发生变化，故(10)、(11)处应分别填入 202.205.3.130 和 80。

【问题 4】

考查 Internet 协议属性参数的配置情况。由于网关地址为 192.168.0.254/24，故工作站 A 的 IP 地址，即(12)处在 192.168.0.1～192.168.0.253 范围内任选一个即可。子网掩码为 255.255.255.0，默认网关地址为 192.168.0.254，参照网络结构，可选的 DNS 服务器只有 61.103.110.151。

答案：

【问题 1】

(1) Router1　(2) Switch2　(3) Switch1　(4) Switch2

【问题 2】

(5) 千兆光纤　(6) 百兆双绞线　(7) 千兆双绞线

【问题 3】

(8) 61.103.110.101　(9) 65534

(10) 202.205.3.130　(11) 80

【问题 4】

(12) 在 192.168.0.1～192.168.0.253 范围内均正确

(13) 255.255.255.0　(14) 192.168.0.254

(15) 61.103.110.151

例 3　阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2007 年 5 月下午试题一)

【说明】

某办公室只有一台主机 host1 接入 Internet，其 TCP/IP 协议属性如图 1-38 所示。

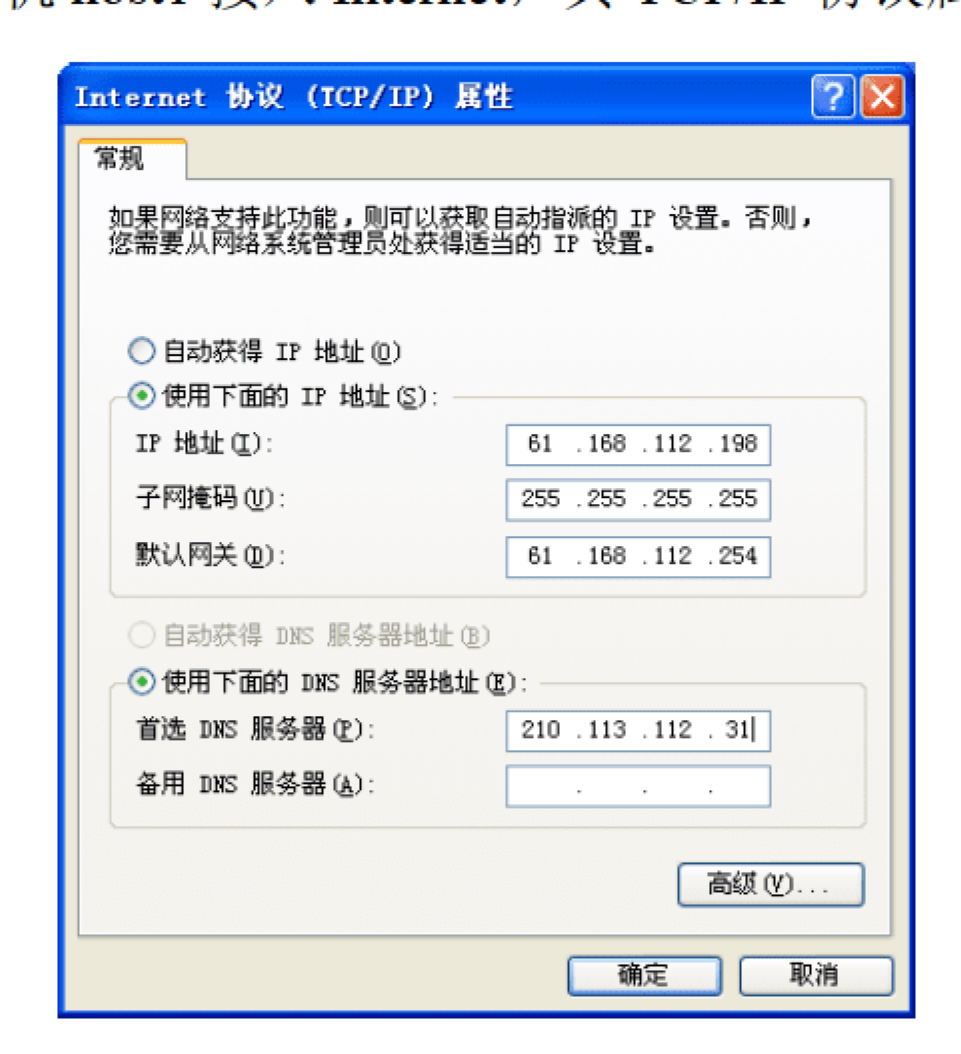


图 1-38　【Internet 协议(TCP/IP)属性】对话框

在没有增加公网 IP 地址的情况下，增加几台主机共享网络连接接入 Internet，其拓扑结构如图 1-39 所示，host1 eth0 网卡的 Internet 协议属性如图 1-40 所示。

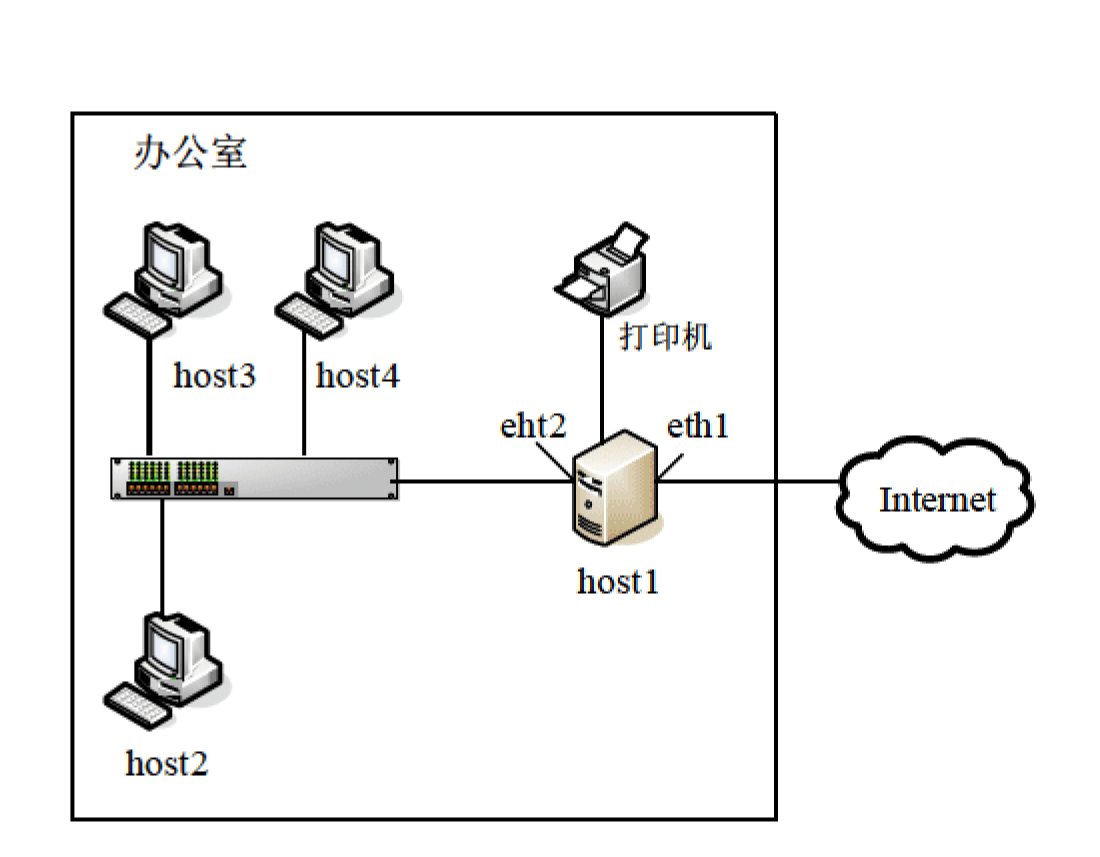



图 1-39　网络拓扑结构图

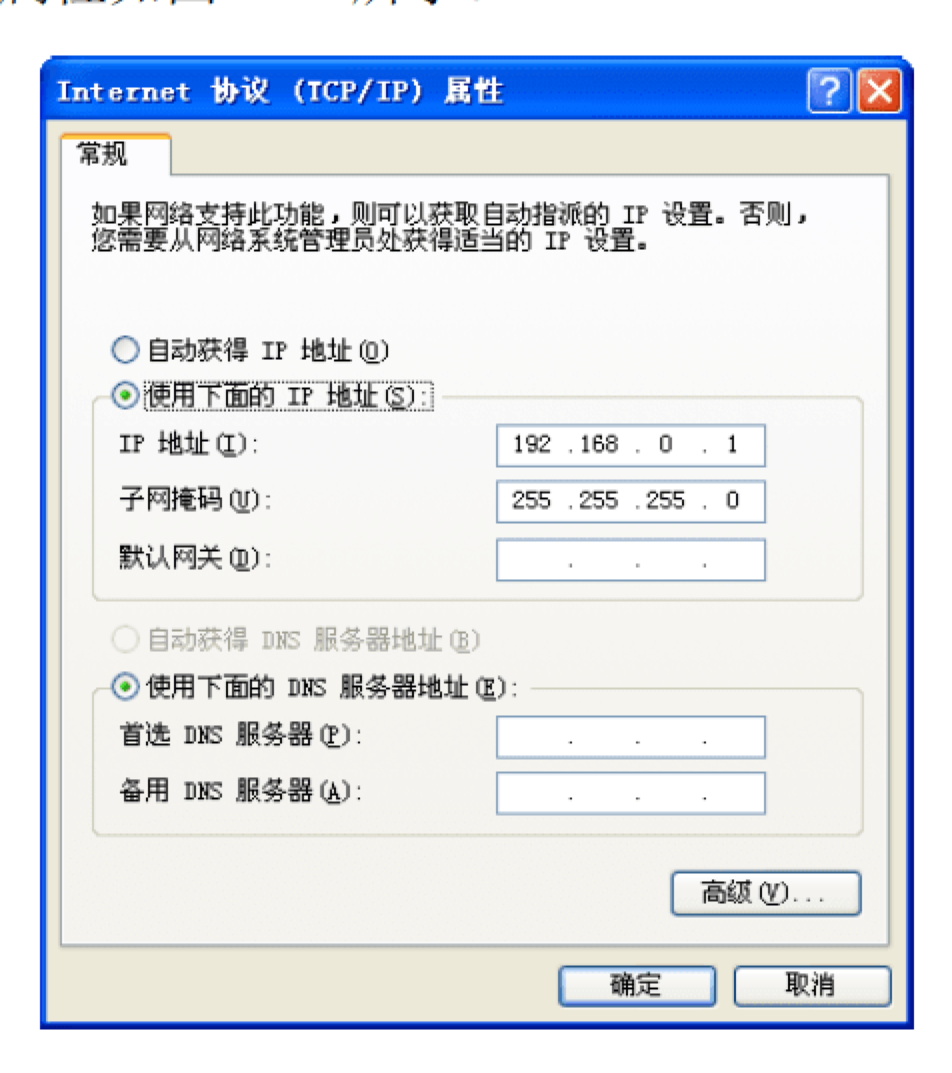


图 1-40　【Internet 协议(TCP/IP)属性】对话框

【问题 1】(3 分)

为了保证其他主机能接入 Internet，在如图 1-41 所示的 host1 eth1 网卡“Internet 连接共享”应如何选择？



图 1-41　【本地连接　属性】对话框

【问题 2】(4 分)

请为图 1-39 中的 eth1 网卡配置 Internet 协议属性参数。

IP 地址：　　　　　(1)

子网掩码：　　　　(2)

默认网关：　　　　(3)

首选 DNS 服务器：　(4)

【问题 3】(6 分)

请为图 1-39 中 host2 配置 Internet 协议属性参数。

IP 地址： (5) (范围) (2 分)

子网掩码： (6) (1 分)

默认网关： (7) (1 分)

首选 DNS 服务器： (8) (2 分)

【问题 4】(2 分)

若 host2 的 IP 地址设为 192.168.0.188，其发送到 Internet 上的 IP 数据包的源 IP 地址为 (9) 。

分析：

【问题 1】

这是一道有关局域网组建的题目。题中主机 host1 作为代理服务器，办公室内其他主机通过 host1 的外网卡接入 Internet。主机 host1 的外网卡的【本地连接 属性】对话框中应选中【允许其他网络用户通过此计算机的 Internet 连接来连接】复选框。可允许其他主机通过主机 host1 接入 Internet。

【问题 2】

在新建的网络中，主机 host1 的外网卡 eth1 直接与 Internet 相连，使用的是全局 IP 地址，因此保持原来的设置即可。

【问题 3】

host1 的内网卡 eth0 的 IP 地址为 192.168.0.1，host2、host3、host4 与 eth0 都在组建的局域网内部，IP 地址应在同一网段上，范围为 192.168.0.2～192.168.0.254，子网掩码为 255.255.255.0。

由于所有主机都是通过 host1 接入 Internet，可知 host2 的默认网关为 host 的内网卡 eht0，IP 地址为 192.168.0.1。局域网内部没有 DNS 服务器，因此 host2 的首选 DNS 服务器应与 host1 一致，为 210.113.112.31。

【问题 4】

若 host2 发送数据包在到达 host1 之前为 192.168.0.188，到达 Internet 后转换为 host1 外网卡的地址，故为 61.168.112.198。

答案：

【问题 1】

选中【允许其他网络用户通过此计算机的 Internet 连接来连接】复选框。

【问题 2】

(1) 61.168.112.198 (2) 255.255.255.0

(3) 61.168.112.254 (4) 210.113.112.31

【问题 3】

(5) 192.168.0.2～192.168.0.254 范围内均可

(6) 255.255.255.0 (7) 192.168.0.1

(8) 210.113.112.31

【问题 4】

(9)　61.168.112.198

例 4　阅读以下说明，回答问题 1～问题 2，将解答填入答题纸对应的解答栏内。(2006 年 11 月下午试题一 问题 1～问题 2)

【说明】

某校园网络拓扑结构如图 1-42 所示。

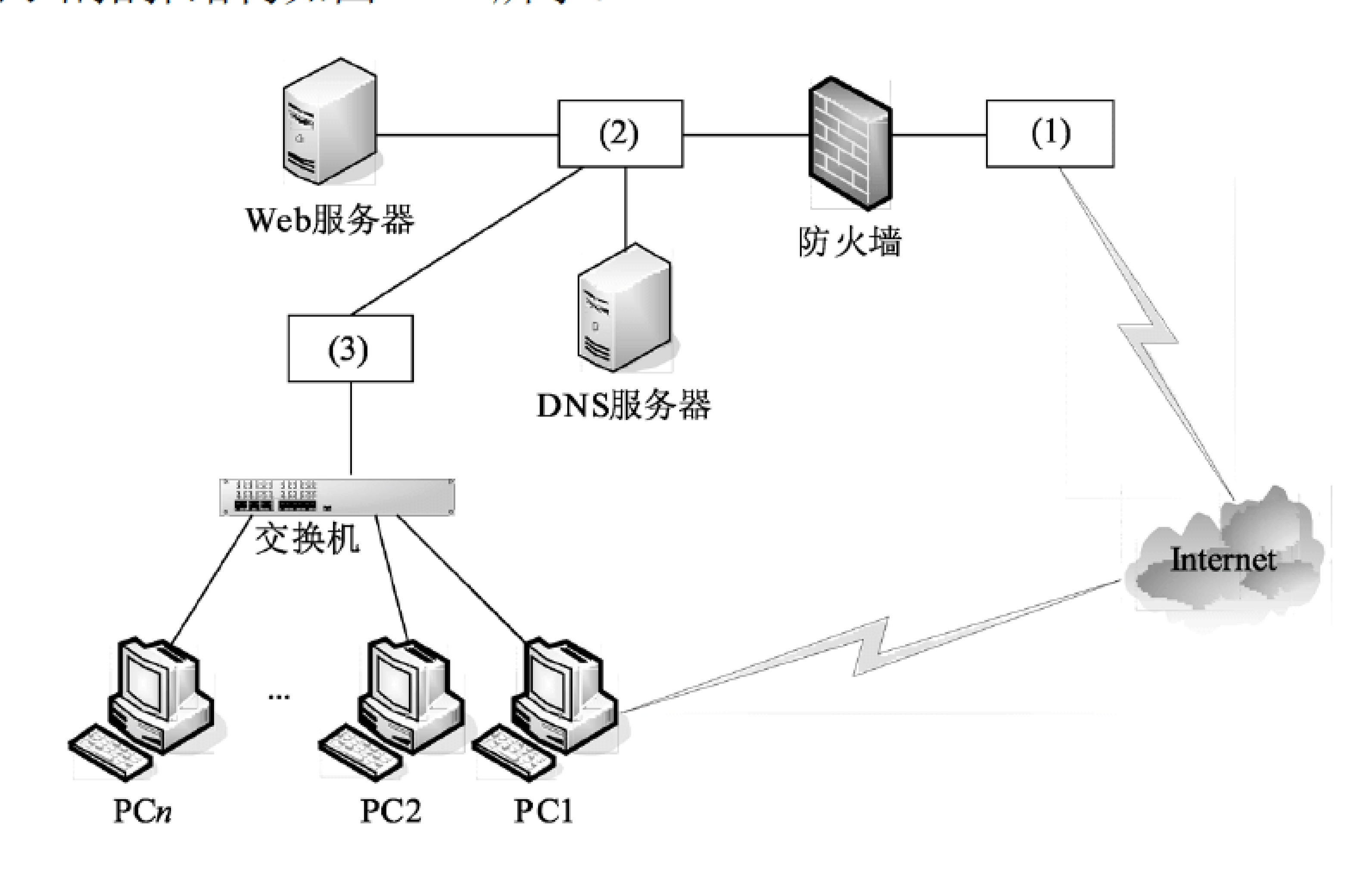


图 1-42　某校园的网络拓扑结构图

【问题 1】(3 分)

从备选设备中为图 1-42 中的(1)～(3)处选择合适的设备名称，填入答题纸对应的解答栏内。

备选设备：汇聚交换机　核心交换机　路由器

【问题 2】(2 分)

将管理终端的串口与交换机的__(4)__相连，通过超级终端可对交换机进行基本配置。

A. 控制台端口　　　　B. 以太网接口

C. 串口　　　　　　　D. 广域网接口

分析：

【问题 1】

层次化网络设计可有效地将全局通信问题分解考虑，就如同软件工程中的结构化程序设计一样，其中，分层设计核心层的功能主要是实现骨干网络之间的优化传输，负责整个网络的网内数据交换。核心层设计任务的重点通常是冗余能力、可靠性和高速的传输。核心层一直被认为是流量的最终承受者和汇聚者，所以要求核心交换机拥有较高的可靠性和性能。汇聚层主要负责连接接入层结点和核心层中心，汇集分散的接入点，扩大核心层设备的端口密度和种类，汇聚各区域的数据流量，实现骨干网络之间的优化传输。汇聚交换机还负责本区域内的数据交换，一般与中心交换机类型相同，仍需要较高的性能和比较丰富的功能，但吞吐量较低。接入层网络作为二层交换网络，提供工作站等设备的网络接入。接入层在整个网络中接入交换机的数量最多，具有即插即用的特性。对此类交换机的要求：

一是价格合理；二是可管理性好，易于使用和维护；三是要有足够的吞吐量；四是稳定性好，能够在比较恶劣的环境下稳定地工作。

因此，(1)～(3)处依次应填入路由器、核心交换机、汇聚交换机。

【问题 2】

通常对一台新的交换机进行配置和管理有两个大的步骤：一是通过仿真终端进行 IP 地址设置，二是通过浏览器进行管理。

用一条 RS-232 电缆将管理终端的串口与交换机的控制台端口(Console)相连，然后使用【附件】中的【超级终端】命令即可。因此，(4)处应选 A。

答案：

【问题 1】

(1) 路由器　　(2) 核心交换机　　(3) 汇聚交换机

【问题 2】

(4) A

例 5　阅读以下说明，回答问题，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题一)

【说明】

某公司总部和三个子公司分别位于四处，其网络结构如图 1-43 所示，公司总部和各子公司所需主机数如表 1-14 所示。

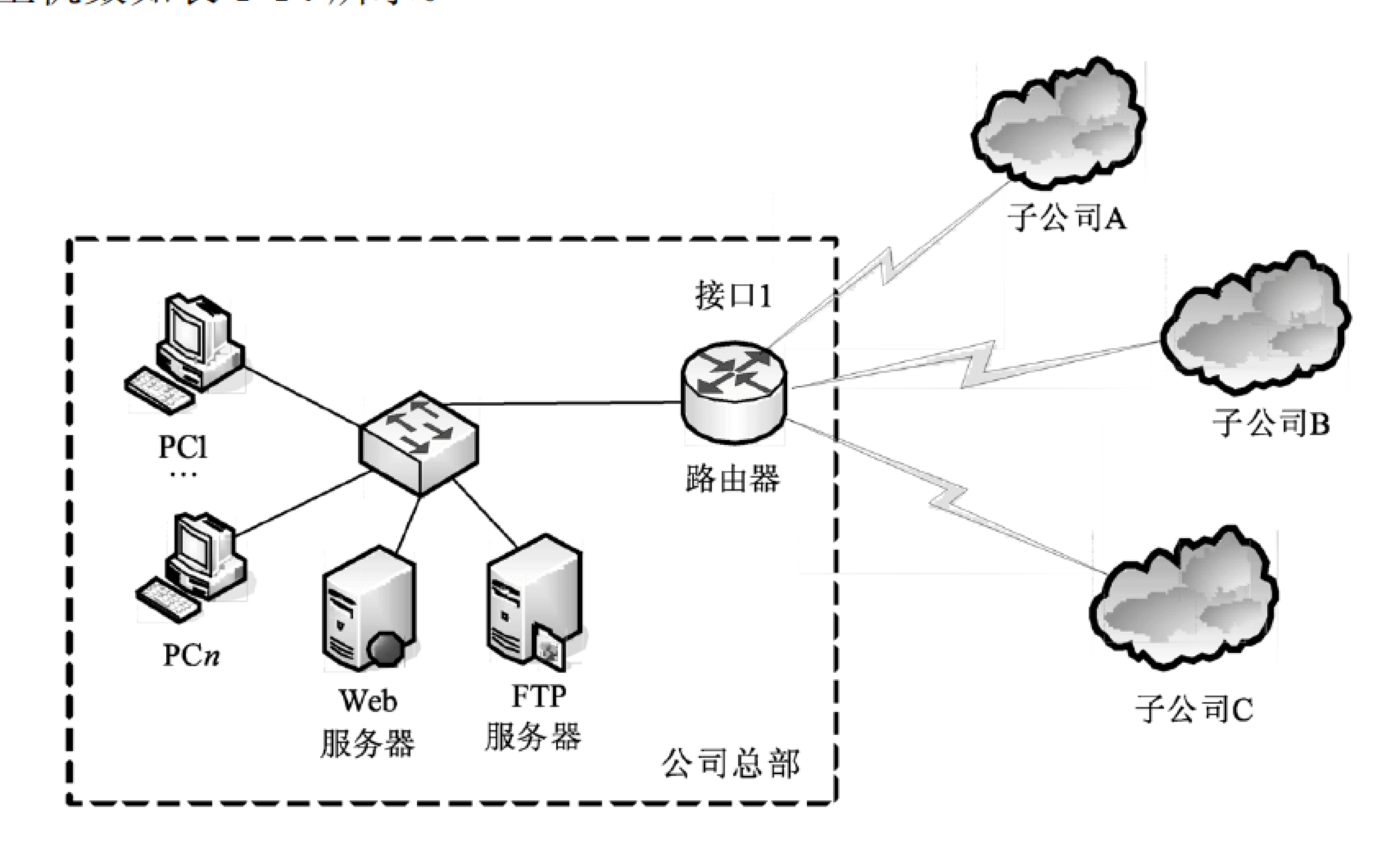


图 1-43　某公司与其子公司网络互连示意图

表 1-14　公司总部与各子公司的主机数

部　门	主机数量/台
公司总部	50
子公司 A	25
子公司 B	10
子公司 C	10

【问题 1】(6 分)

该公司用一个 C 类地址块 202.119.110.0/24 组网，将表 1-15 中的(1)～(6)处空缺的主机地址或子网掩码填写在答题纸的相应位置。

表 1-15　IP 地址规划

部　门	可分配的地址范围	子网掩码
公司总部	202.119.110.129～(1)	255.255.255.192
子公司 A	(2)～202.119.110.94	(3)
子公司 B	202.119.110.97～(4)	255.255.255.240
子公司 C	(5)～(6)	255.255.255.240

分析：

对于空(1)和空(4)是给出一台主机的 IP 和子网掩码，求该子网的可分配置的主机范围，这里直接给出子网的网络地址和广播地址。

公司总部：网络地址是 202.119.110.128，广播地址是 202.119.110.191。

子公司 B：网络地址是 202.119.110.96，广播地址是 202.119.110.111。

对于空(2)和空(3)，子公司 A 有 20 台主机，需要确定子网掩码和主机范围。我们知道子网划分的原理是从主机号“借”位作为子网号的，该公司用一个 C 类地址，其默认的网络号为 24 位，主机号为 8 位，现要借位作子网号，借多少位呢？由于子公司 A 有 20 台主机，则主机号至少需要 5 位，这是因为 24−2<20<25−2。也就是说，最多从主机号中借 3 位作为子网号，这样网络号和子网号共 27 位，因此子网掩码为 1111 1111.1111 1111. 1111 1111.1110 000，即 255.255.255.224，这就是空(3)要填写的内容。子网掩码确定后，就很容易计算出该子网的网络地址和广播地址了，分别为 202.119.110.64、202.119.110.95，从而得到空(2)为 202.119.110.65。

对于空(5)和空(6)，需要确定子公司 C 的子网主机范围。也许读者会认为，只要在 202.119.110.0/24 这个网络中随便找一段没有用的地址块，使它的子网掩码为 255.255.255.240 即可。其实不然。本题划分子网的思路是这样的：将这个 C 类用 26 位子网掩码(即 255.255.255.192)划分成 4 个子网，每个子网的地址是 64 个(含网络地址和广播地址)，但由于全 0 和全 1 子网不能使用，只有中间的两个子网可以使用，因此其中一个分配给公司总部，另一个再一分为二，一个用于子公司 A，另一个用于子公司 B 和子公司 C，划分过程如图 1-44 所示。

答案：

(1) 202.119.110.190

(2) 202.119.110.65

(3) 255.255.255.224

(4) 202.119.110.110

(5) 202.119.110.113

(6) 202.119.110.126

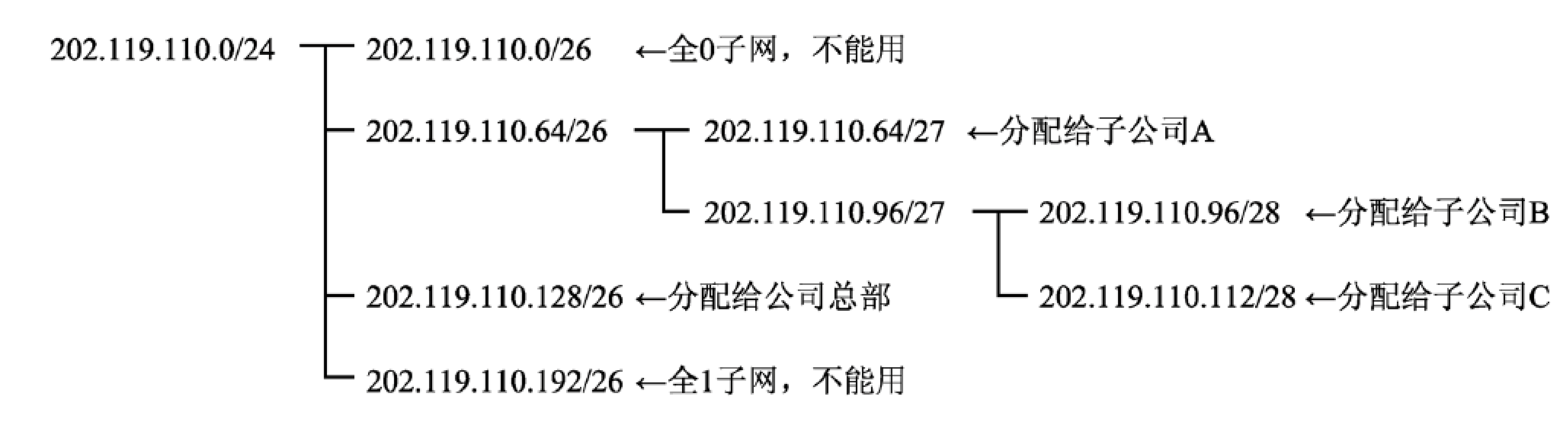


图 1-44　IP 地址规划过程

1.6.3　同步练习

阅读以下说明，回答问题 1～问题 3，将解答填入对应的答案栏内。

【说明】

随着网络应用的日益广泛，接入网络和边缘网络的需求也更加复杂多样，企业为了开展电子商务，必须实现与 Internet 的互联，路由器是实现这一互联的关键设备，路由器可以为企业提供越来越多的智能化服务，包括安全性、可用性和服务质量(QoS)等。

下面是某公司，VLSM(Variable Length Subnet Mask，可变长子网掩码)子网的设计方法。假设该公司被分配了一个 C 类地址，该公司的网络拓扑结构如图 1-45 所示。其中部门 A 拥有主机数 20、部门 B 拥有主机数 10、部门 C 拥有主机数 20、部门 D 拥有主机数 10。分公司 A 拥有主机数 10、分公司 C 拥有主机数 10。假设分配的网络为 192.168.1.0。

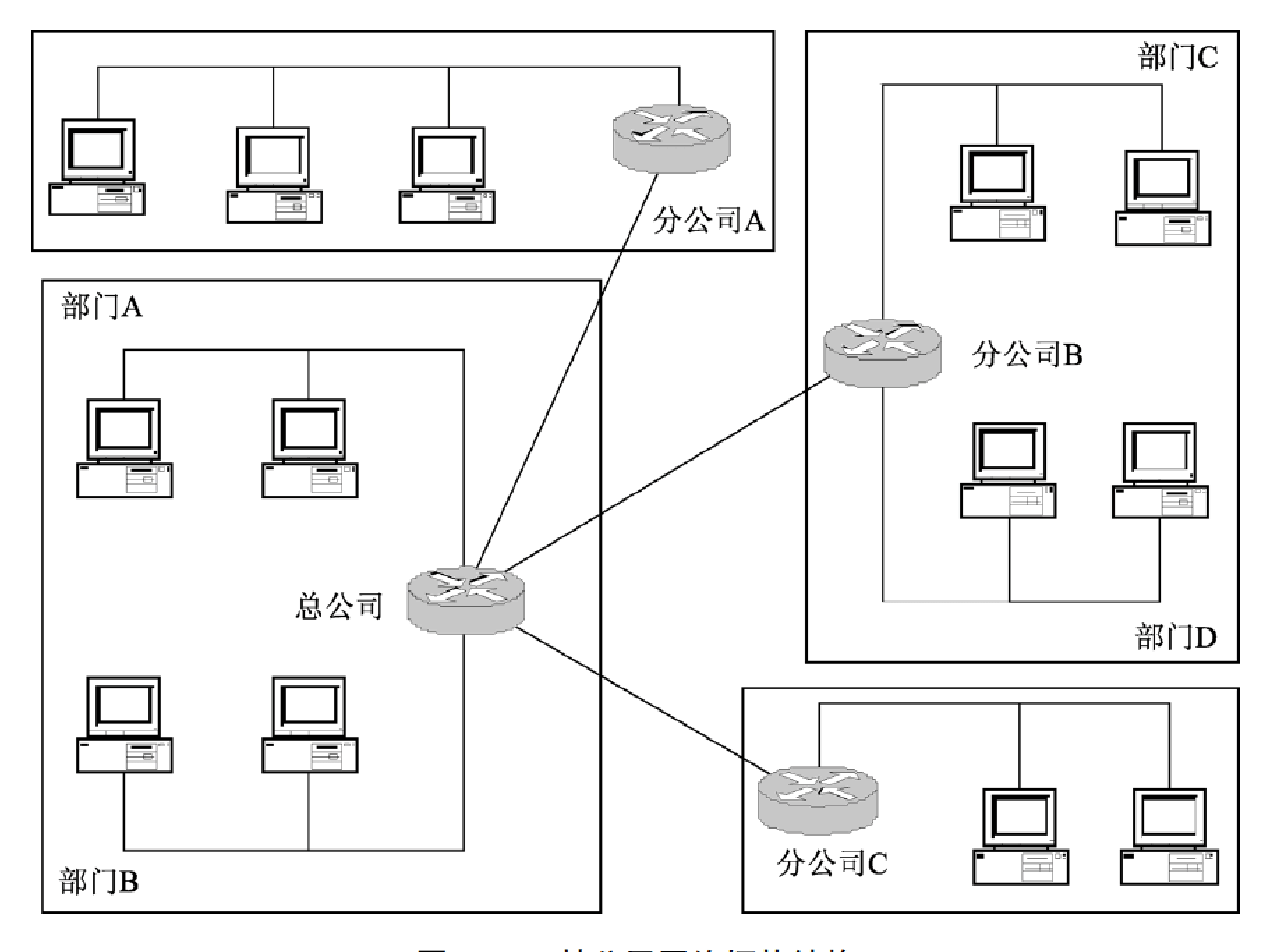


图 1-45　某公司网络拓扑结构

【问题 1】请为该网络进行子网分割，至少有 3 个不同变长的子网掩码，请列出您所求的变长子网掩码，并说明理由。注意：该单位的路由器不支持全 0 和全 1 子网。

【问题 2】请列出您所分配的网络地址。

【问题 3】为该网络分配广域网地址。

1.6.4　同步练习参考答案

【问题 1】255.255.255.224、255.255.255.240、255.255.255.252。划分过程如图 1-46 所示。(注：划分的方法很多，下面只是其中的一种。)

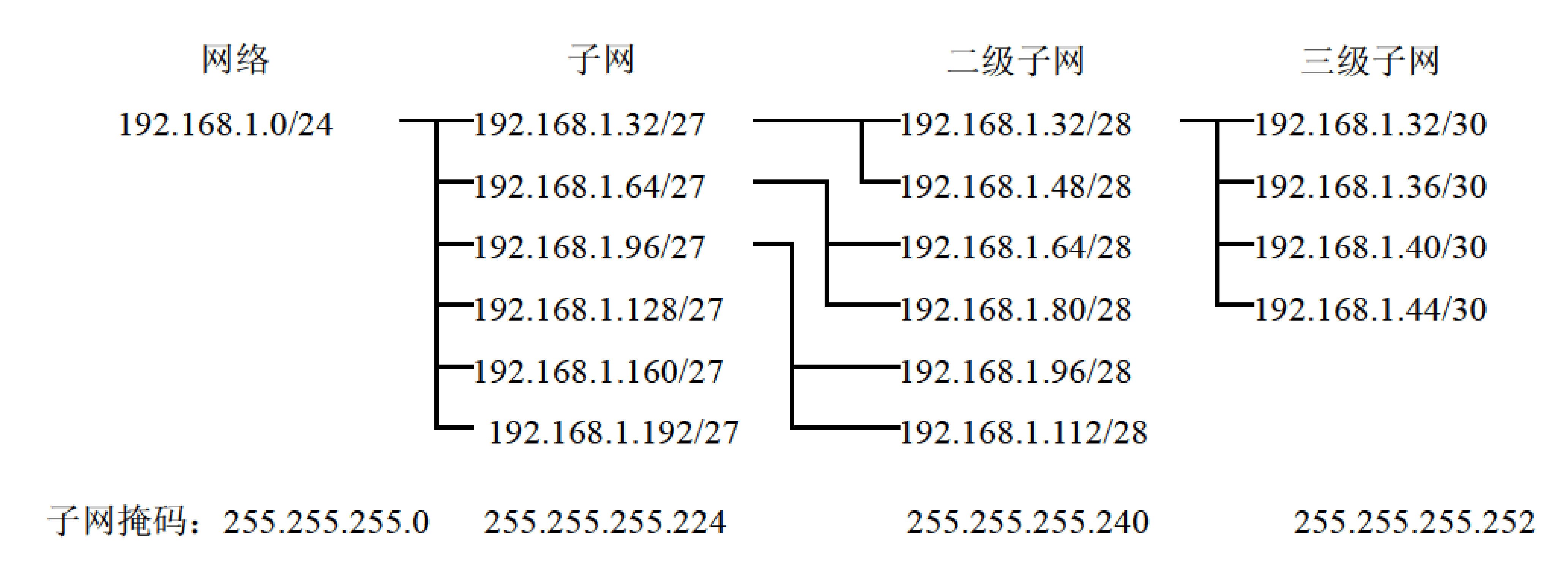


图 1-46　其中一种 IP 地址划分方法

【问题 2】将 192.168.1.48/28 分配给部门 B、192.168.1.64/28 分配给部门 D、192.168.1.80/28 分配给分公司 A、192.168.1.96/28 分配给分公司 C、192.168.1.112/28 保留为网络扩展、192.168.1.128/27 分配给部门 A、192.168.1.160/27 分配给部门 C、192.168.1.192/27 保留为网络扩展。

【问题 3】

把 192.168.1.33 和 192.168.1.34 分配给部门 A 和分公司 A 之间的串行线路；

把 192.168.1.37 和 192.168.1.38 分配给部门 A 和部门 C 之间的串行线路；

把 192.168.1.33 和 192.168.1.34 分配给部门 A 和分公司 C 之间的串行线路；

将 192.168.1.44/30 子网中的 192.168.1.45 和 192.168.1.46 保留为网络扩展。

1.7　本 章 小 结

本章知识点在 2009 年的新大纲中变化较大，增加了交换机和路由器的配置以及网络接入服务知识点，弱化了综合布线的考核要求。

这部分内容主要要求考生掌握局域网的设计步骤、局域网的设备选型、综合布线、交换机的部署和配置、子网的划分方法以及综合布线系统的设计。要求考生综合上述知识，根据用户需求，合理利用局域网设备和技术设计出符合用户需求的网络。

本章内容为下午科目的重点内容，尤其是 Internet 协议属性配置、交换机的配置和路由

器的配置，在以往的试题中曾多次考到。

1.8　达标训练题及参考答案

1.8.1　达标训练题

1．阅读以下说明，回答问题 1～问题 3，将答案填入对应的答案栏内。

【说明】

某单位有一个网络，其中有一台主机的 IP 地址是 190.190.147.134。请回答以下问题。

【问题 1】这个地址是一个什么类型的地址？不划分子网时，其网络地址是什么？广播地址是什么？

【问题 2】它的默认子网掩码是什么？

【问题 3】若子网掩码是 255.255.240.0，则这台主机所在的子网地址是什么？该子网的广播地址是什么？这个 IP 地址所在的子网的主机 IP 地址范围是什么？

2．阅读以下说明，回答问题 1～问题 4，将解答填入对应的答案栏内。

【说明】

某公司申请了一个 C 类地址 196.102.56.0，公司有生产部门、市场部门、财务部门、人事部门、技术部门和经理办公室，每个部门都需要划分为单独的网络，即需要划分至少 5 个子网，每个子网至少支持 24 台主机(使用固定子网掩码)。

【问题 1】将子网掩码设置为什么？

【问题 2】每个子网有多少个主机地址？

【问题 3】196.102.56.197 所在子网的网络地址是什么？

【问题 4】196.102.56.197 所在子网的广播地址是什么？

3．阅读以下说明，回答问题 1～问题 3，将解答填入对应的答案栏内。

【说明】

某一小型公司从 ISP 申请了一个 Internet 出口，ISP 给该公司提供了 5 个 IP 地址，分别是 222.34.109.66～222.34.109.70，ISP 给该公司提供的路由器地址是 222.34.109.65。

【问题 1】由于 ISP 忘记了告诉子网掩码，你认为最有可能的子网掩码是什么？

【问题 2】这个子网的子网地址是什么？

【问题 3】这个子网的广播地址是什么？

1.8.2　参考答案

1．

【问题 1】B 类地址、190.190.0.0、190.190.255.255

【问题 2】255.255.0.0

【问题 3】190.190.144.0、190.190.159.255、190.190.144.1～190.190.159.254

2.

【问题 1】255.255.255.224

【问题 2】30

【问题 3】196.102.56.192

【问题 4】196.102.56.223

3.

【问题 1】255.255.255.248

【问题 2】222.34.109.64

【问题 3】222.34.109.71

第 2 章　局域网服务器的安装和配置

大纲要求：

- IP 地址、子网掩码的规划配置
- Windows Web 服务器的配置和维护
- Windows DNS 服务器的配置和维护
- Windows 电子邮件服务器的配置和维护
- Windows FTP 服务器的配置和维护
- Windows 代理服务器的配置和维护
- Windows DHCP 服务器的配置和维护

2.1　操作系统的安装

2.1.1　考点辅导

2.1.1.1　Windows Server 2003 安装程序

1. Windows Server 2003 安装方式

Windows Server 2003 不再支持从软盘引导安装操作系统，其安装光盘不再提供引导软盘。Windows Server 2003 操作系统提供 Winnt.exe 和 Winnt32.exe 两个安装程序。其中 Winnt.exe 用来在文本模式下安装操作系统，Winnt32.exe 用来在窗口模式下安装操作系统。在运行 Windows Server 2003 操作系统的安装程序前，必须运行 Smartdrv 加载高速缓存，否则，Windows Server 2003 不能正常安装。Windows Server 2003 主要有以下两种安装方式。

(1)　无人值守安装。Windows Server 2003 可以利用无人值守应答文件 Unattend.txt 将安装过程自动化，系统在安装过程中需要用户交互输入的所有信息都自动通过 Unattend.txt 文件获得。如果不使用 Unattend.txt 文件，则安装过程将要求用户输入以下信息：许可协议，产品密钥，区域和语言选项，可选系统组件，计算机名称和本地管理员密码，时区、日期和时间设置，网络组件，工作组或域选择等。

(2)　复制安装。复制安装通过创建 Windows Server 2003 操作系统的映像，然后将映像文件恢复到多台目的计算机。复制安装不但可以部署 Windows Server 2003 操作系统，还可以将应用程序和系统配置信息复制到其他目的计算机，从而节省部署操作系统和应用程序的时间，提高系统部署效率。运行 Windows Server 2003 操作系统的计算机在网络中通过安全标识符(Security Identifiers，SID)而不是计算机名管理和控制，在复制安装时必须通过相应的工具删除源计算机在网络中必须惟一的信息(如 SID)，然后创建源计算机的映像，确保利用映像文件部署的目的计算机能够在网络中正常运行。Windows Server 2003 提供了 Sysprep.exe 工具用来删除网络中每台计算机必须惟一的特有信息。Windows Server 2003 操

作系统不提供磁盘复制工具部署操作系统，必须借助第三方工具(如 Symantec Ghost)实现 Windows Server 2003 操作系统的复制安装。

2. Windows Server 2003 的配置

Windows Server 2003 的配置主要包括：修改计算机名、管理本地用户与组、维护网络服务(包括添加、删除和管理服务)、配置网络协议、终端服务和配置文件服务器等。

1)　修改计算机名

计算机名修改可以通过打开控制面板中的【系统】管理器操作完成，同时也可以设置计算机的隶属关系，可以设置为隶属于域或工作组。

2)　管理本地用户与组

使用【本地用户和组】命令，可以创建并管理存储在本地计算机上的用户和组，主要是利用管理工具中的【计算机管理】窗口进行相关操作。

3)　添加、删除与管理网络服务

默认条件下 Windows Server 2003 并不安装任何的网络服务，系统安装成功后，用户可以通过【管理您的服务】和【添加删除程序】两种方式来添加、删除或管理网络服务。

4)　配置网络协议

正确安装网卡驱动和网络协议，并正确配置 IP 地址信息，是服务器与网络计算机进行正常通信的基础。配置网络协议，主要是指配置 TCP/IP 协议，包括 IP 地址、子网掩码、默认网关、DNS 和 WINS 等设置。

5)　配置文件服务器

文件服务器提供并管理文件的访问，可以通过【管理您的服务器】中的【添加或删除角色】命令来选择【文件服务器】进行配置。

6)　终端服务

终端服务提供了通过作为终端仿真器工作的【瘦客户机】软件远程访问服务器桌面的能力。终端服务器基本由 3 部分技术组成，即客户端部分、协议部分及服务器端部分。客户端和服务器通过远程桌面协议进行通信。其工作方式为，与终端服务相距很远的客户端用户可以像坐在终端服务器前一样执行操作和使用远程终端服务。客户端把键盘输入、鼠标移动和鼠标单击信息发给终端服务；终端服务得到这些信息后，在终端服务的会话内完成所需的操作，然后将更新后的信息发送回客户端。

终端服务器默认情况下没有安装，需要进行手动添加。终端服务的安装有两种方式：一种是使用【配置您的服务器向导】快速安装，另一种是使用【添加或删除程序】安装。选择【开始】|【管理工具】|【终端服务配置】命令，在打开的【终端服务配置】对话框中双击右侧窗格中的 RDP-Tcp 连接。在【RDP-Tcp 属性】对话框中可进行赋予用户权限、更改加密级别、允许用户自动登录到服务器、配置终端服务超时和重新连接、管理远程控制等配置。

2.1.1.2　安装 Red Flag Server 4.0

(1)　启动 Linux 安装程序。可以选择从光盘、硬盘或 NFS 进行安装。完成安装引导进入图形化安装界面后，可以根据提示选择安装类型，即【安装红旗操作系统】或【恢复系统引导】。

(2) 配置分区。配置内容包括：分区的命名设计、分区的组织、选择分区方式(【用 Disk Druid 手工分区】或用【Fdisk 程序手工分区】)和确认要格式化的分区等，可以根据系统应用使用 RAID 和 LVM 技术。

① 分区的命名。Linux 通过字母和数字的组合来识别硬盘分区。命名规则：前两个字母表示分区所在的设备类型；第三个字母表示分区在哪个设备上；数字表示分区的次序。例如，/dev/hda3 是指第一个 IDE 硬盘上的第三个主分区或扩展分区。

② 分区的组织。安装 Red Flag Server 4.0 至少需要创建根分区和交换分区。根分区是 Linux 根文件系统驻留的地方；交换分区主要用来支持虚拟内存的交换空间，其大小建议设置为计算机内存的 1 ~ 2 倍之间。

③ 软 RAID 配置。RAID 称为独立磁盘冗余阵列。RAID 的基本思想是：把多个便宜的小磁盘组合到一起，成为一个磁盘组，使性能达到或超过一个容量巨大、价格昂贵的磁盘。采用 RAID 技术加快了磁盘速度，扩充了存储能力，具有高效恢复磁盘的功能。RAID 一般分为 RAID0、RAID1、RAID4、RADI5 和线性 RAID。可以采用硬件 RAID 或软件 RAID 的方式来实现 RAID。

④ LVM 配置。LVM 为计算机提供了更高层次的磁盘存储解决方案，使系统管理员可以方便地分配存储空间。Red Flag 可以根据需要将一个或多个物理盘分区创建为用于 LVM 的物理卷，已创建的软件 RAID 设备也可以设置为物理卷。

(3) 配置引导。LILO 是 Red Flag Server 4.0 的启动引导程序，它支持 Red Flag Server 4.0 与多种操作系统共存，允许用户在系统启动时通过 LILO 菜单选择想要进入的操作系统。可以把 LILO 安装在 MBR(主引导记录)或者引导分区的第一个扇区。MBR 是硬盘上的一个特别的区域，会自动被 BIOS 装载，是引导装载程序控制引导进程最早的位置。建议尽可能地把 LILO 安装在主引导扇区内。

(4) 配置用户。安装程序会提示设置系统的 root 密码，必须输入一个根口令，否则安装无法继续；接下来可以建立一个或多个普通用户帐号并为其设置口令。

(5) 安装和复制文件。完成用户设置后，会进入安装确认界面。确认相关安装信息后，安装程序会读取需要安装的软件包信息，进行必要的准备工作，然后开始文件的复制过程。

(6) 创建引导盘。引导盘会存储当前的系统设置，在系统出现问题时帮助用户引导和还原 Red Flag Server 4.0 系统，对于系统维护和故障排除具有重要的意义。

安装成功后，单击【退出】按钮，将弹出的光盘取出，然后重新启动系统，即完成系统的安装。

2.1.2 典型例题分析

例 1 阅读以下说明，回答问题 1～问题 2，将解答填入答题纸对应的解答栏内。(2008 年 5 月下午试题三)

【说明】

Linux 是一个类 UNIX 的操作系统，其功能强大，适合构建网络服务平台，提供 DNS、WWW、FIT、NAT 等服务。

【问题 1】(3 分)

在安装 Linux 前，必须对硬盘进行分区。在 Linux 系统中用设备名称指定分区，命名方法是在驱动器的设备名称(/dev/had 或/dev/hdb)后加上指定分区的数字，1～4 代表主分区，逻辑分区从 5 开始编号。

若某系统使用两个 IDE 硬盘，第一个硬盘 a 分为 3 个分区，其中一个为主分区，另外两个为逻辑分区；第二个硬盘 b 分为 5 个分区，其中两个为主分区，另外 3 个为逻辑分区。那么硬盘 a 的主分区设备名为__(1)__，硬盘 b 的第三个逻辑分区的设备名为__(2)__。

系统安装完成后，需要配置网卡。/etc/sysconfig/__(3)__是网络配置文件，提供 IP 地址、域名、网关等信息。

【问题 2】(4 分)

Linux 支持多分区结构，依据分区功能填写表 2-1 中的空(4)～(7)。

表 2-1　分区功能表

分　区	功　能
__(4)__	包含所有用户的主目录
__(5)__	根目录
__(6)__	交换分区
__(7)__	存放临时文件

分析：

【问题 1】

Linux 通过字母和数字的组合来标识硬盘分区。前两个字母表示分区所在的设备类型，hd 表示 IDE 分区，sd 表示 SCSI 分区。第三个字母表示分区在哪个设备上，如 hda 对应第一块 IDE 硬盘，sdc 对应第三块 SCSI 硬盘。数字表示分区次序，数字 1～4 表示主分区或扩展分区，逻辑分区从 5 开始，如 5 表示第一逻辑分区，6 表示第二逻辑分区等。

题目中系统使用两个 IDE 硬盘，第一个硬盘 a 分为 3 个分区，其中一个为主分区，另外两个为逻辑分区，则主分区设备名为/dev/hda1，两个逻辑分区的设备名分别为/dev/hda5 和/dev/hda6；第二个硬盘 b 分为 5 个分区，其中两个为主分区，另外 3 个为逻辑分区，则两个主分区设备名分别为/dev/hdb1 和/dev/hdb2，3 个逻辑分区的设备名分别为/dev/hdb5、/dev/hdb6 和/dev/hdb7。

/etc/sysconfig/network 文件是用来指定服务器上的网络配置信息的，包括了控制和网络有关的文件和守护程序行为的参数，如 HOSTNAME=hostname hostname 表示服务器的主机名，GATEWAY=gw-ip gw-ip 表示网络网关的 IP 地址等。

【问题 2】

Linux 支持多分区结构，根分区(/)是根文件系统驻留的地方，是整个系统的基础。交换分区(swap)用来支持虚拟内存的交换空间，当没有足够的内存来处理系统数据时，就要使用交换分区的空间。/home 分区包含所有用户的主目录，几乎可以保存所有的用户文件。/tmp 分区用来存放临时文件。

答案：

【问题 1】

(1) /dev/hda1　　(2) /dev/hdb7　　(3) network

【问题 2】

(4) /home　　(5) /或 root　　(6) swap

(7) /tmp

2.1.3 同步练习

阅读以下关于 Linux 网卡安装和配置过程的说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某个采用动态 IP 地址分配策略的计算机使用了最新的 BCM 5751 网卡芯片，由于 Red Hat Linux 9 操作系统无法自动识别此硬件，需要单独安装驱动程序才能正常工作。安装过程如下。

(1) 将驱动程序压缩文件 bcm5700-8.3.14.tar.gz 复制到一个临时目录中，并使用解压缩命令将驱动程序包 bcm5700-8.3.14.tar.gz 解压缩。

(2) 用 make 命令构建驱动程序的可加载模块。

(3) 用 make install 命令加载驱动程序。

(4) 重新启动系统，启动过程中系统找到网卡进行相应参数配置。

【问题 1】(2 分)

将文件 bcm5700-8.3.14.tar.gz 解压缩的命令是__(1)__。

A. rar　　B. tar　　C. unzip　　D. rpm

【问题 2】(3 分)

打开/etc/sysconfig/network 文件，内容如下：

```
NETWORKING=__(2)__
HOSTNAME=localhost.localdomain
```

打开并编辑网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth0，内容如下：

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=__(3)__
USERCTL=no
PEERDNS=yes
TYPE=Ethenet
```

从备选答案中为(2)和(3)空缺处选择恰当内容，填入答题纸对应的解答栏内。

A. yes　　B. no　　C. dhcp　　D. auto

【问题 3】(3 分)

在/etc/sysconfig/network-scripts/目录中有许多脚本命令，运行该目录下的__(4)__命令，可以启动该网卡，该命令的命令行参数是__(5)__(填空)。

A. ifdown　　　　B. ifup　　　　C. netdown　　　　D. netup

【问题 4】(5 分)

可以使用程序 (6) 来查看网络接口的运行情况，输出如下：

```
eth0 Link encap:Ethernet  Hwaddr:00:12:3F:94:E7:B9
inet addr:192.168.0.63  Bcast: (7) Mast: (8)
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:1501  errors:0  dropped:0  overruns:0  frame:0
TX packets:74  errors:0  dropped:0  overruns:0  carrier:0
collisions:0  txqueuelen:100
RX bytes:164444 (160.5 Kb)  TX bytes:9167 (8.9 Kb)
Interrupt:11  Memory:dfcf0000-dfd00000
```

上述输出表明，该网卡运行 (9) (填正常或不正常)；上文中 MTU 的含义是 (10) 。

【问题 5】(2 分)

运行 route-n 命令，可以输出路由选择表如下：

```
Kernel  IP  routing  table
Destination  Gateway     Genmask        Flags  Metric  Ref  Use  Iface
192.168.0.0  0.0.0.0      255.255.255.0    U      0      0    0    eth0
169.254.0.0  0.0.0.0      255.255.0.0      U      0      0    0    eth0
127.0.0.0    0.0.0.0      255.0.0.0        U      0      0    0    lo
0.0.0.0      192.168.0.1  0.0.0.0          UG     0      0    0    eth0
```

则该网络的默认网关地址是 (11) 。

2.1.4　同步练习参考答案

【问题 1】

(1) B

【问题 2】

(2) A　　　　(3) C

【问题 3】

(4) B　　　　(5) eth0

【问题 4】

(6) ifconfig

(7) 192.168.0.255

(8) 255.255.255.0

(9) 正常

(10) 最大传输单元

【问题 5】

(11) 192.168.0.1

2.2 DNS 服务器配置

2.2.1 考点辅导

2.2.1.1 Windows Server 2003 下 DNS 服务器的安装与配置

1. 安装 DNS 服务

在 Windows Server 2003 默认安装时，DNS 服务并没有安装。这里要注意作为 DNS 服务器的计算机必须有静态 IP 地址和子网掩码，并设置自己的 IP 地址为首选 DNS 服务器。例如，服务器的 IP 地址和子网掩码为 192.168.10.10 和 255.255.255.0，则本机的 DNS 服务器地址中首选 DNS 服务器地址必须设为 192.168.10.10 或 127.0.0.1。

在 Windows Server 2003 计算机上安装 DNS 服务器的步骤如下。

(1) 在要安装 DNS 服务的 Windows Server 2003 计算机上选择【开始】|【设置】|【控制面板】命令，在【控制面板】窗口中，双击【添加/删除程序】选项，选择【添加/删除 Windows 组件】命令，在打开的对话框的【组件】列表框中选中【网络服务】复选框，如图 2-1 所示。

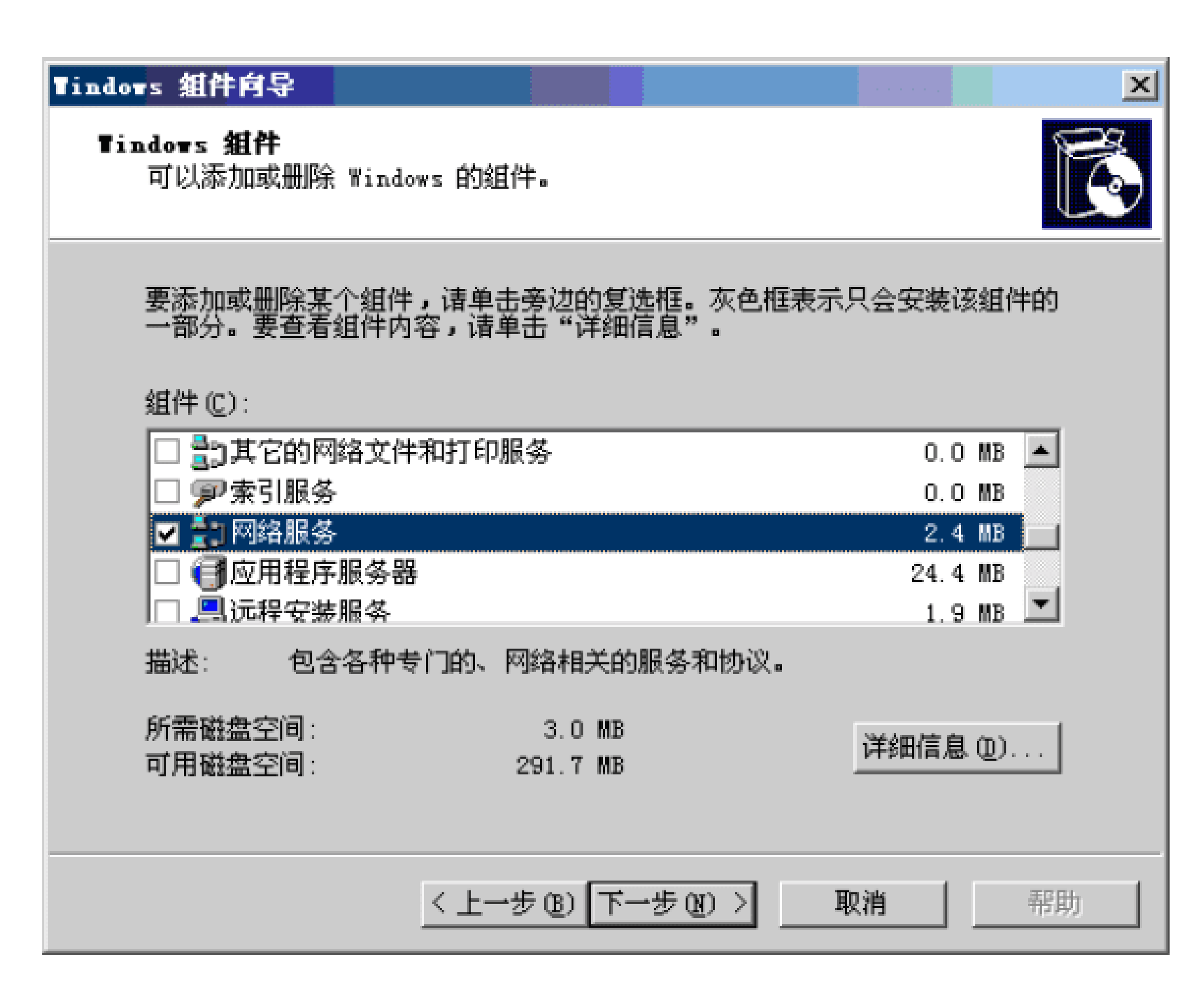


图 2-1 【Windows 组件向导】对话框

(2) 单击【详细信息】按钮，出现【网络服务】对话框，选中【域名系统(DNS)】复选框，如图 2-2 所示。

(3) 单击【确定】按钮，返回上一个对话框，再单击【下一步】按钮则开始安装 DNS 服务器。

2. 配置计算机成为 DNS 服务器的客户端

其具体步骤如下。

(1) 在客户端计算机上打开【Internet 协议(TCP/IP)属性】对话框，选中【使用下面的

DNS 服务器地址】单选按钮，在【首选 DNS 服务器】文本框中输入 DNS 服务器 IP 地址，如 192.168.10.10。如果网络中还有其他的 DNS 服务器可供选择的话，则在【备用 DNS 服务器】文本框中输入其他 DNS 服务器 IP 地址，如图 2-3 所示。

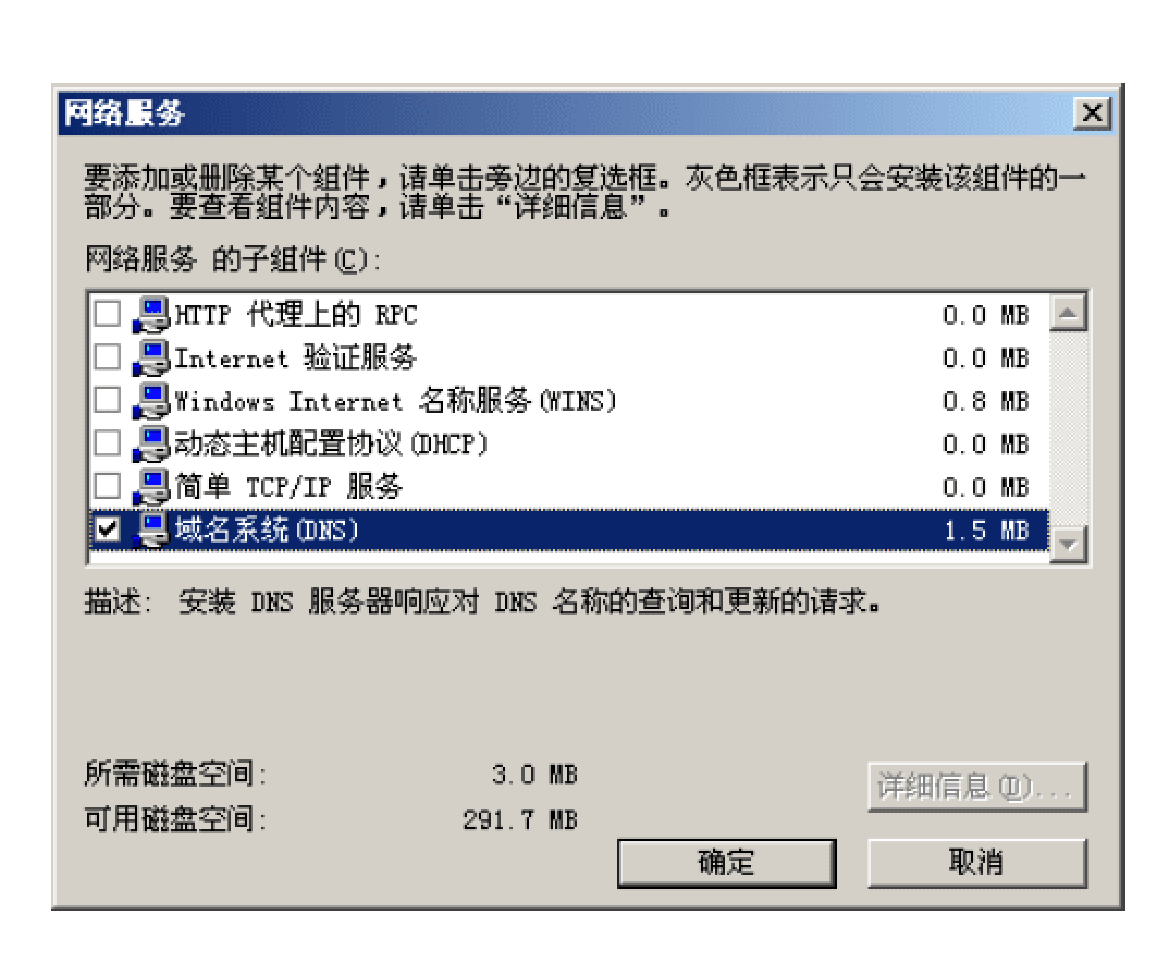


图 2-2 【网络服务】对话框

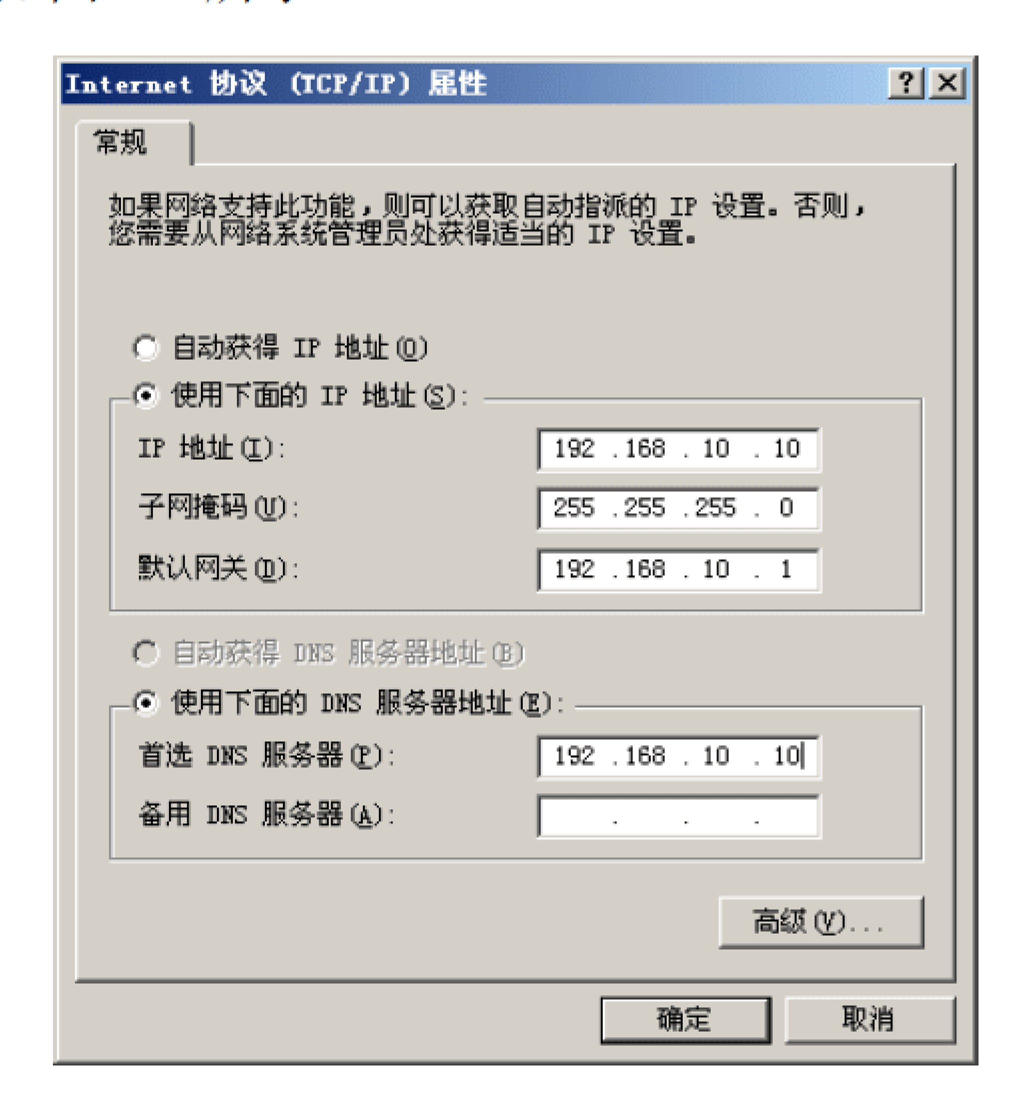


图 2-3　设置 DNS 服务器的 TCP/IP 属性

(2)　单击【确定】按钮，即完成对 DNS 客户端的设置。

3.　创建 DNS 正向解析区域

必须在 DNS 服务器内创建区域与区域文件，以便位于该区域内的主机数据存储到区域文件内。

Windows Server 2003 的 DNS 服务器支持下述 3 种区域类型。

- 标准主要区域：用来存储此区域内所有主机数据的正本。其区域文件采用 DNS 规格的一般文本文件标准。当在 DNS 服务器创建一个主要区域与区域文件后，这个 DNS 服务器就成为主域名服务器。
- 标准辅助区域：用来存储此区域内所有主机数据的副本，这份数据是从其主要区域利用区域传送的方式复制过来的。存储此数据的区域文件也是采用 DNS 规格的一般文本文件标准，但它是只读的，不能被修改。当在 DNS 服务器内创建一个辅助区域后，这个 DNS 服务器就是这个区域的辅助名称服务器。
- Active Directory(活动目录)集成区域：只能创建在有活动目录的网络环境中，将此区域的主机数据存储在域控制器的活动目录内，这份数据会自动被复制到其他域控制器内。

Windows Server 2003 的 DNS 服务器有两种查找区域。

- 正向查找区域：可以让 DNS 客户端利用主机的域名查询其 IP 地址。
- 反向查找区域：可以让 DNS 客户端利用 IP 地址查询主机的域名。

创建 DNS 正向解析区域的步骤如下。

(1)　在 DNS 服务器上，依次选择【开始】|【程序】|【管理工具】|DNS 命令，打开 DNS 控制台，如图 2-4 所示。

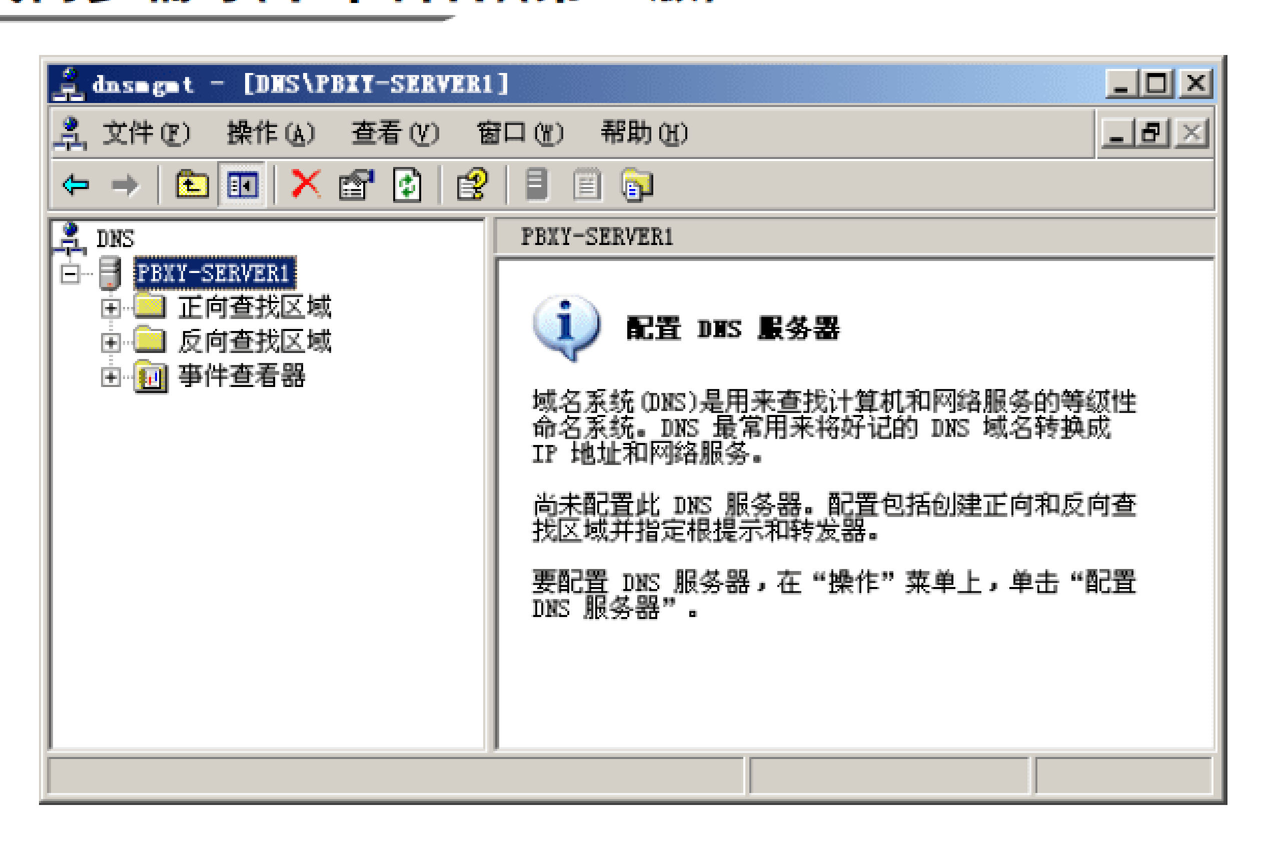


图 2-4　DNS 控制台

(2) 右击【正向查找区域】选项，选择【创建新区域】命令，打开【新建区域向导】对话框，如图 2-5 所示。



图 2-5 【新建区域向导】对话框

(3) 单击【下一步】按钮，在【区域类型】界面中，选中【主要区域】单选按钮，如图 2-6 所示。

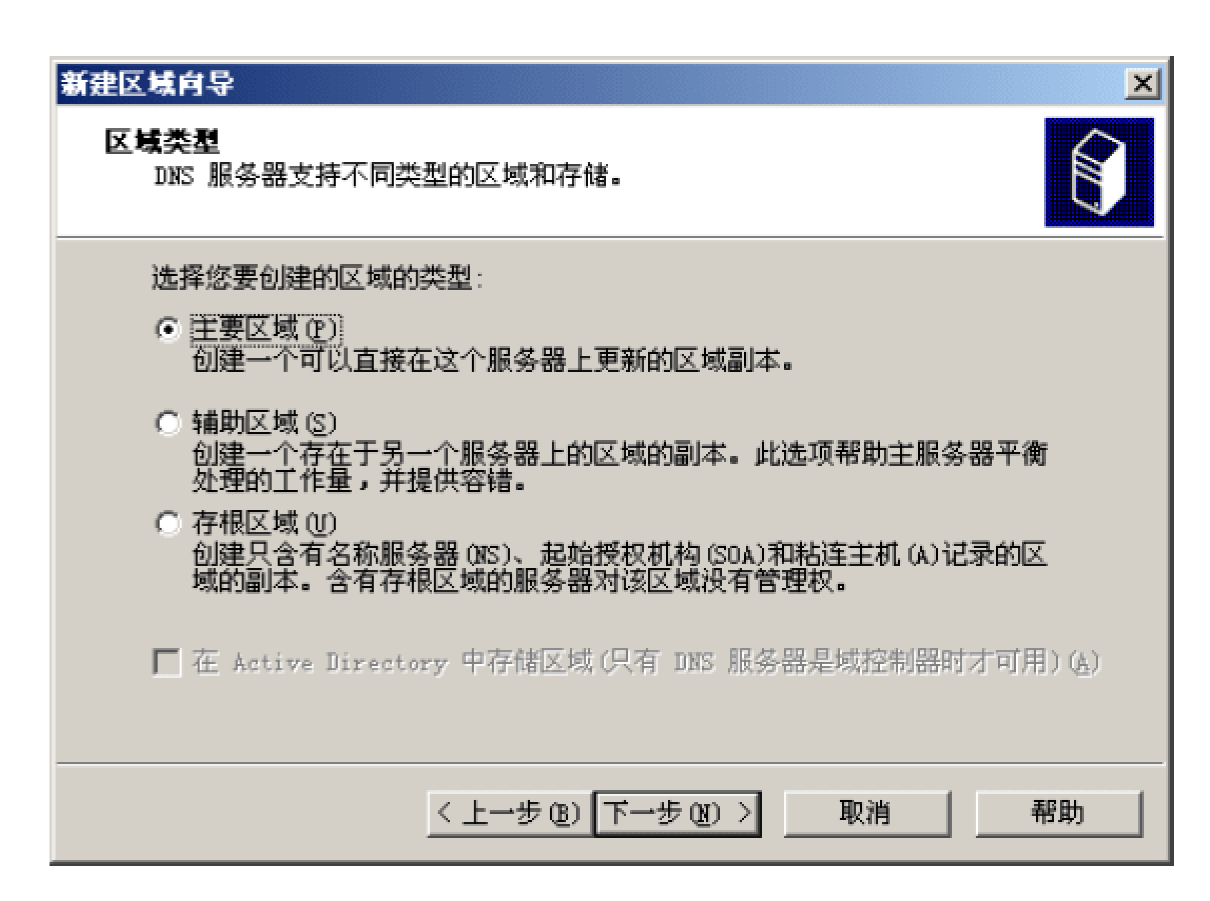


图 2-6 【区域类型】界面

(4) 单击【下一步】按钮，打开【区域名称】界面。在【区域名称】文本框中，为此区域设置名称，如 abc.com.cn，如图 2-7 所示。

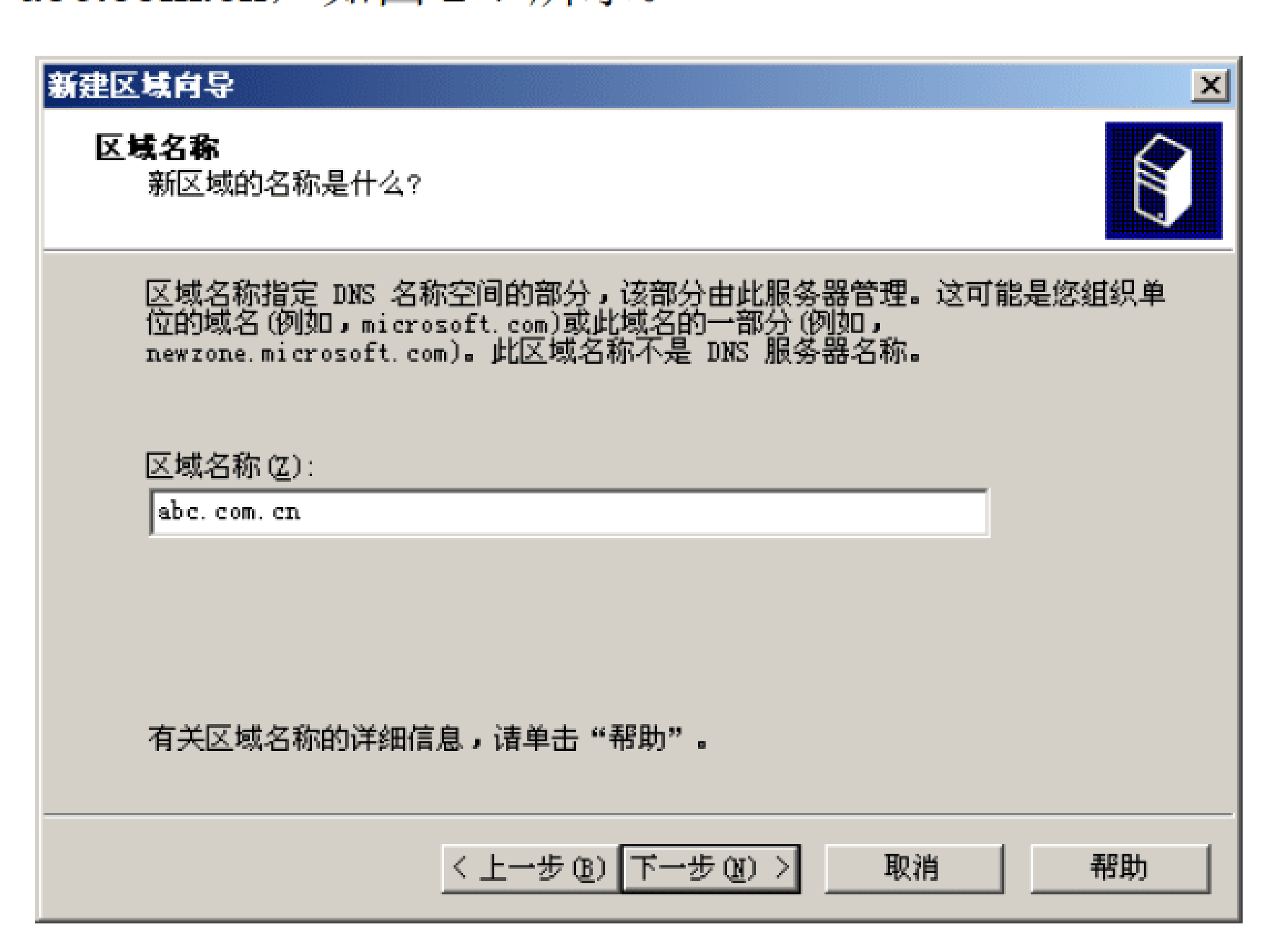


图 2-7 【区域名称】界面

(5) 单击【下一步】按钮，打开【区域文件】界面。在该界面中，可以设置区域文件名(新建文件时)，系统会自动在区域名称后加.dns 作为文件名，也可以使用一个已有文件，如图 2-8 所示。

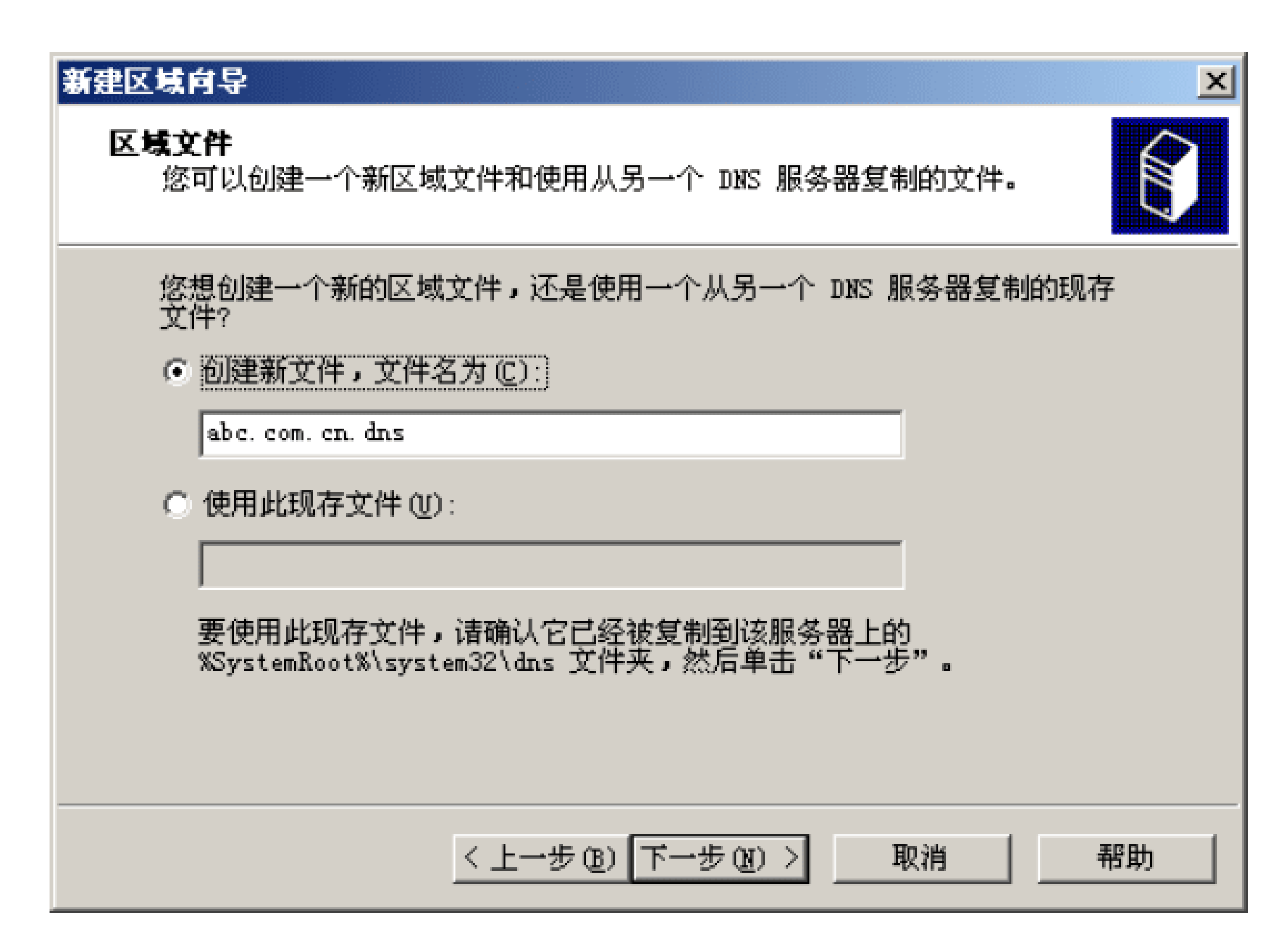


图 2-8 【区域文件】界面

(6) 单击【下一步】按钮，打开【动态更新】界面。在此，用户可指定这个 DNS 区域是否允许接受安全或不安全的动态更新，如图 2-9 所示。

(7) 单击【下一步】按钮，打开【正在完成新建区域向导】界面，如图 2-10 所示。在该界面中，系统显示了用户对新建区域进行配置的信息。如果用户认为某项配置需要调整，可单击【上一步】按钮，返回到前面的界面中重新配置；如果确认自己配置正确的话，可单击【完成】按钮，即完成对 DNS 正向解析区域的创建，返回 DNS 控制台以查看区域的状态。



图 2-9 【动态更新】界面



图 2-10 【正在完成新建区域向导】界面

4. 创建 DNS 反向解析区域

反向查找区域可以让 DNS 客户端利用 IP 地址查询其主机的域名，它并不是非常必要，但在某些情况下会用得到。

反向区域中，区域名前半段是其网络 ID 的反向书写，而区域名后半段必须是 in-addr.arpa。例如，如果要针对网络 ID 为 192.168.10.0 的 IP 地址来提供反向解析功能，则此反向区域的名称必须是 10.168.192.in-addr.arpa。

创建 DNS 反向解析区域的步骤如下。

(1) 在 DNS 服务器上，依次选择【开始】|【程序】|【管理工具】|DNS 命令，打开 DNS 控制台，如图 2-4 所示。

(2) 右击【反向查找区域】选项，选择【创建新区域】命令，打开【创建新区域向导】对话框，如图 2-5 所示。

(3) 单击【下一步】按钮，打开【区域类型】界面。在该界面中，选中【主要区域】单选按钮，如图 2-6 所示。

(4) 单击【下一步】按钮，打开【反向查找区域名称】界面。在【网络 ID】文本框中

输入此区域所支持的反向查询的网络 ID，它会自动在【反向查找区域名称】文本框中设置区域名称。也可以直接在【反向查找区域名称】文本框中设置其区域名称。例如，该 DNS 服务器负责 192.168.10.0 这一网络的反向域名解析，可在【网络 ID】文本框中输入 192.168.10，则在【反向查找区域名称】文本框中显示 10.168.192.in-addr.arpa，如图 2-11 所示。

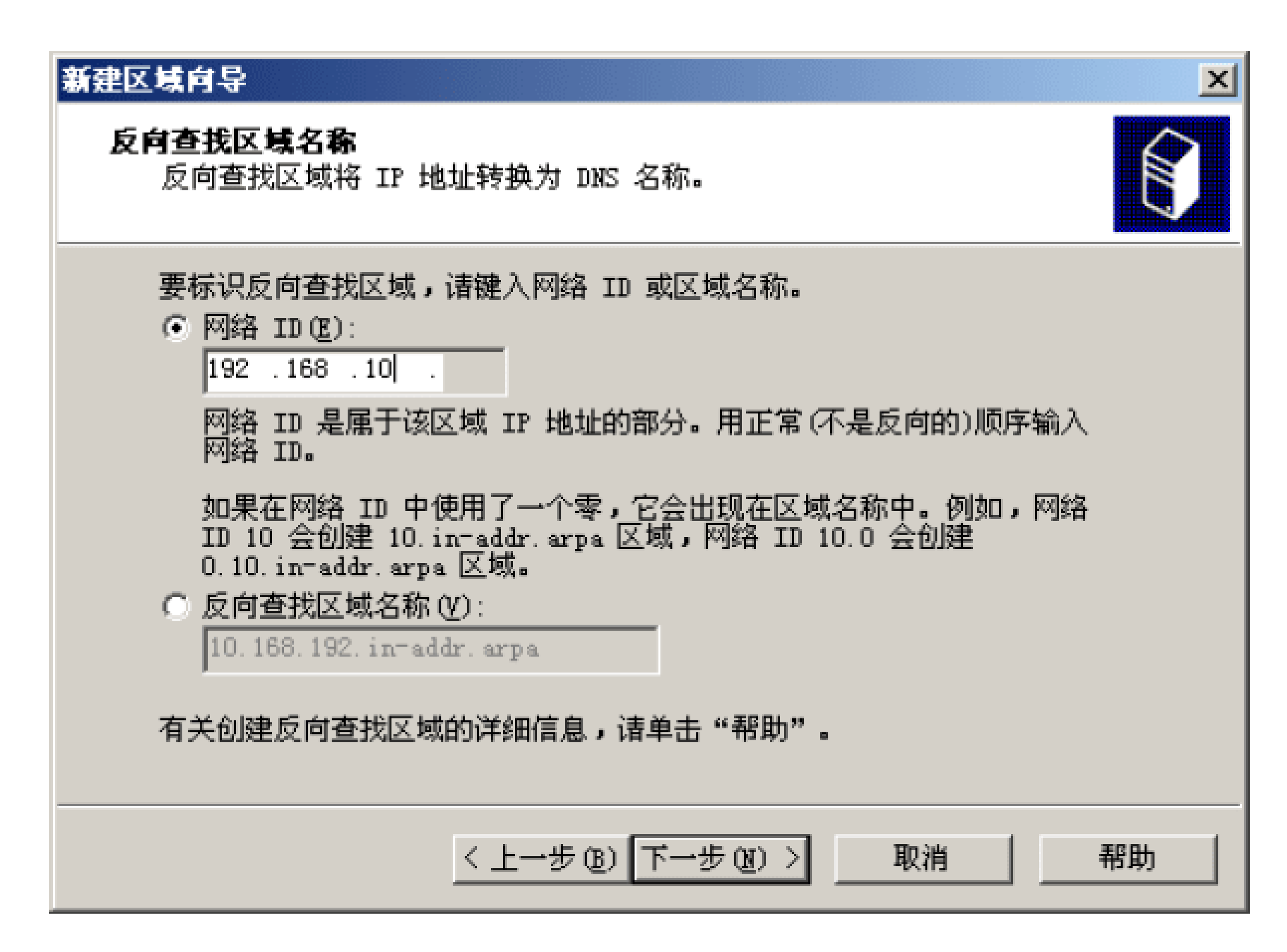


图 2-11 【反向查找区域名称】界面

(5) 单击【下一步】按钮，打开【区域文件】界面。在该界面中，输入区域文件名，系统会自动在区域名称后加.dns 作为文件名并新建一个文件，也可使用一个已有文件，如图 2-12 所示。

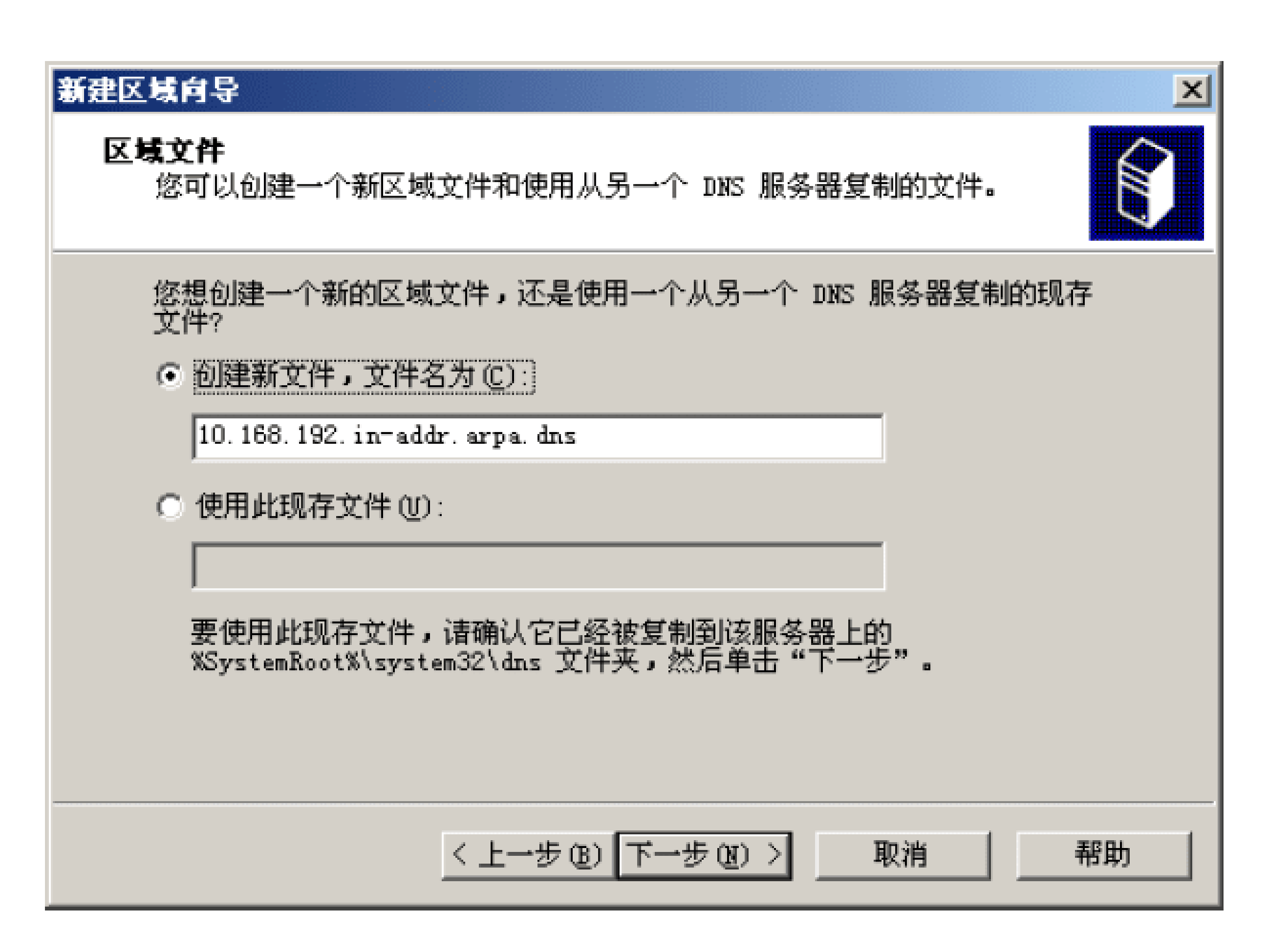


图 2-12 【区域文件】界面

(6) 单击【下一步】按钮，打开【正在完成新建区域向导】界面，如图 2-10 所示。在该界面中，系统显示了用户对新建区域进行配置的信息。如果用户认为某项配置需要调整，可单击【上一步】按钮，返回到前面的界面中重新配置；如果确认自己配置正确的话，可单击【完成】按钮，即完成对 DNS 反向解析区域的创建，返回 DNS 控制台以查看区域的状态。

5. 新建记录到主要区域内

在区域内可以新建主机的相关数据，这些数据被称为资源记录。DNS 服务器支持相当多的资源记录。将数据新建到区域内的具体步骤如下。

(1) 在 DNS 服务器上，依次选择【开始】|【程序】|【管理工具】|DNS 命令，打开 DNS 控制台。

(2) 选择【正向查找区域】中的 abc.com.cn 区域后右击，弹出快捷菜单。根据要新建的记录，在弹出的快捷菜单中选择相应的命令。

- 【新建主机】：将主机的相关数据新建到 DNS 服务器内的区域后，就可以由该 DNS 服务器来实现域名与 IP 地址的映射。选择【新建主机】命令后，打开【新建主机】对话框，如图 2-13 所示。在该对话框中输入主机的主机名与 IP 地址，单击【添加主机】按钮。
- 【新建别名】：在某些情况下，需要为区域内的一台主机创建多个主机名称，例如，一台主机是 Web 服务器同时又是 FTP 服务器，则可以为该主机取两个不同的名称。选择【新建别名】命令后，打开【新建资源记录】对话框，如图 2-14 所示。在该对话框的【别名】选项卡中输入主机的别名和目标主机的完全合格的域名，单击【确定】按钮。



图 2-13 【新建主机】对话框

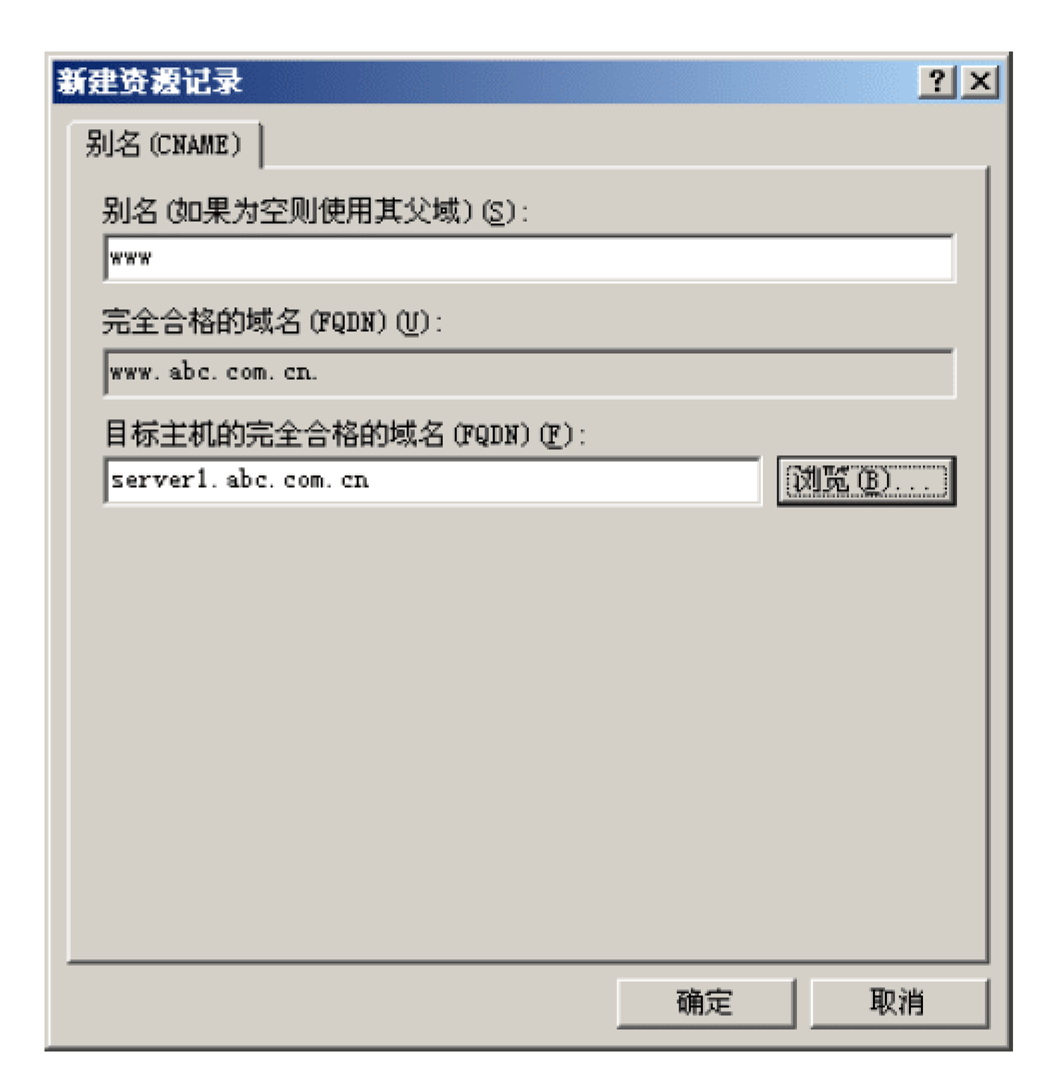


图 2-14 【新建资源记录】对话框

- 【新建邮件交换器】：当用户将邮件送到本地邮件服务器后，本地邮件服务器必须将邮件送到目的地邮件服务器，而目的地的邮件服务器 IP 地址可以向 DNS 服务器查询。邮件交换器记录就是指定哪些主机负责接收该区域的电子邮件，如果在此区域内创建了多个邮件交换器记录，可以设置邮件服务器的优先级，数字较小的优先级较高。选择【新建邮件交换器】命令后，打开【新建资源记录】对话框，如图 2-15 所示。在该对话框的【邮件交换器】选项卡中分别输入【主机或子域】、【邮件服务器的完全合格的域名】及【邮件服务器优先级】，然后单击【确定】按钮。

(3) 选择【反向查找区域】中的 10.168.192.in-addr.arpa 区域后右击，在弹出的快捷菜单中选择【新建指针】选项，打开【新建资源记录】对话框，如图 2-16 所示。在该对话框的【指针】选项卡的【主机 IP 号】文本框中，输入主机 IP 地址的最后一个十进制数，在【主机名】文本框中，输入 DNS 主机的完全合格域名，该计算机使用此指针记录提供反向查找(把 IP 地址解析为域名)。单击【确定】按钮，建立新增的指针。新增的指针记录将显示在主窗口右侧的列表中。

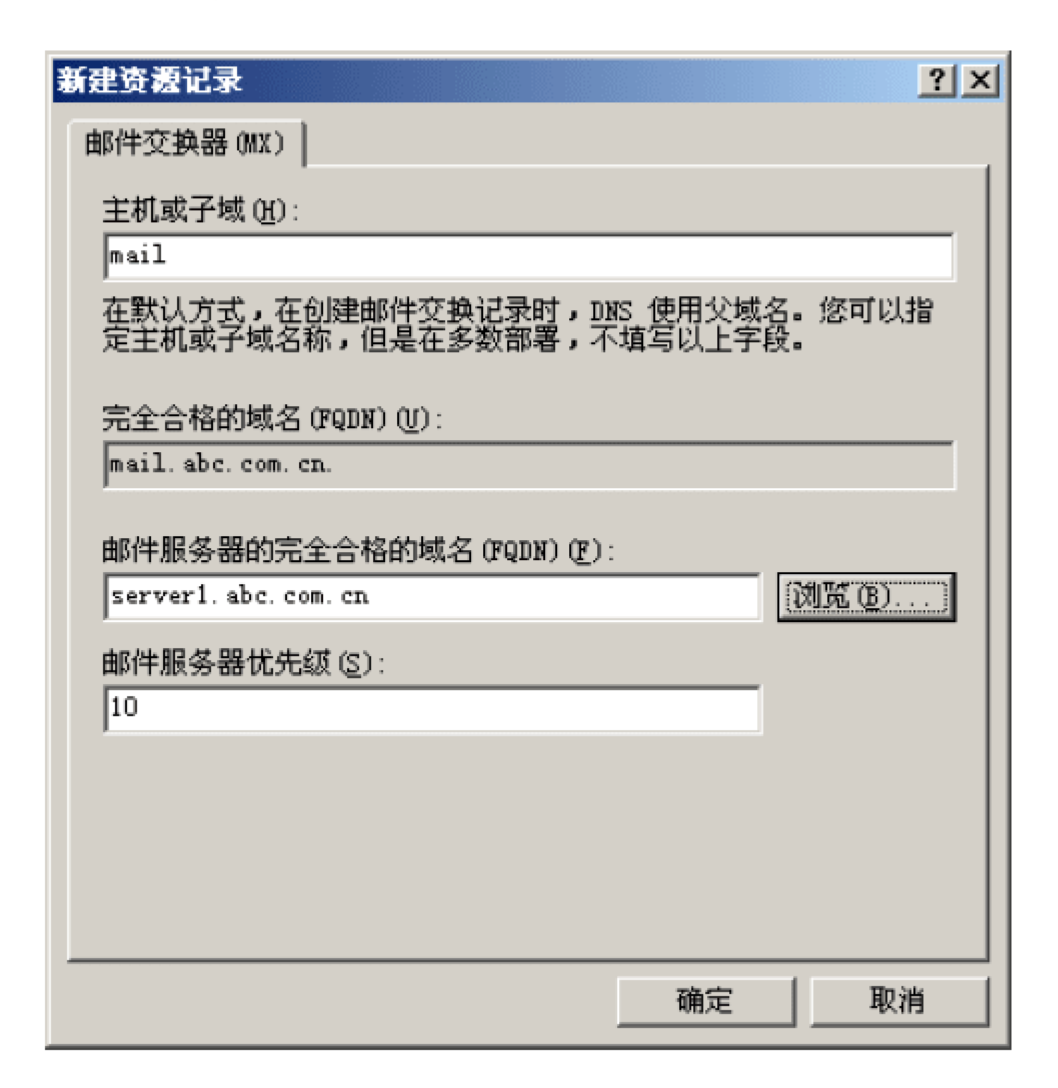


图 2-15　新建邮件交换器

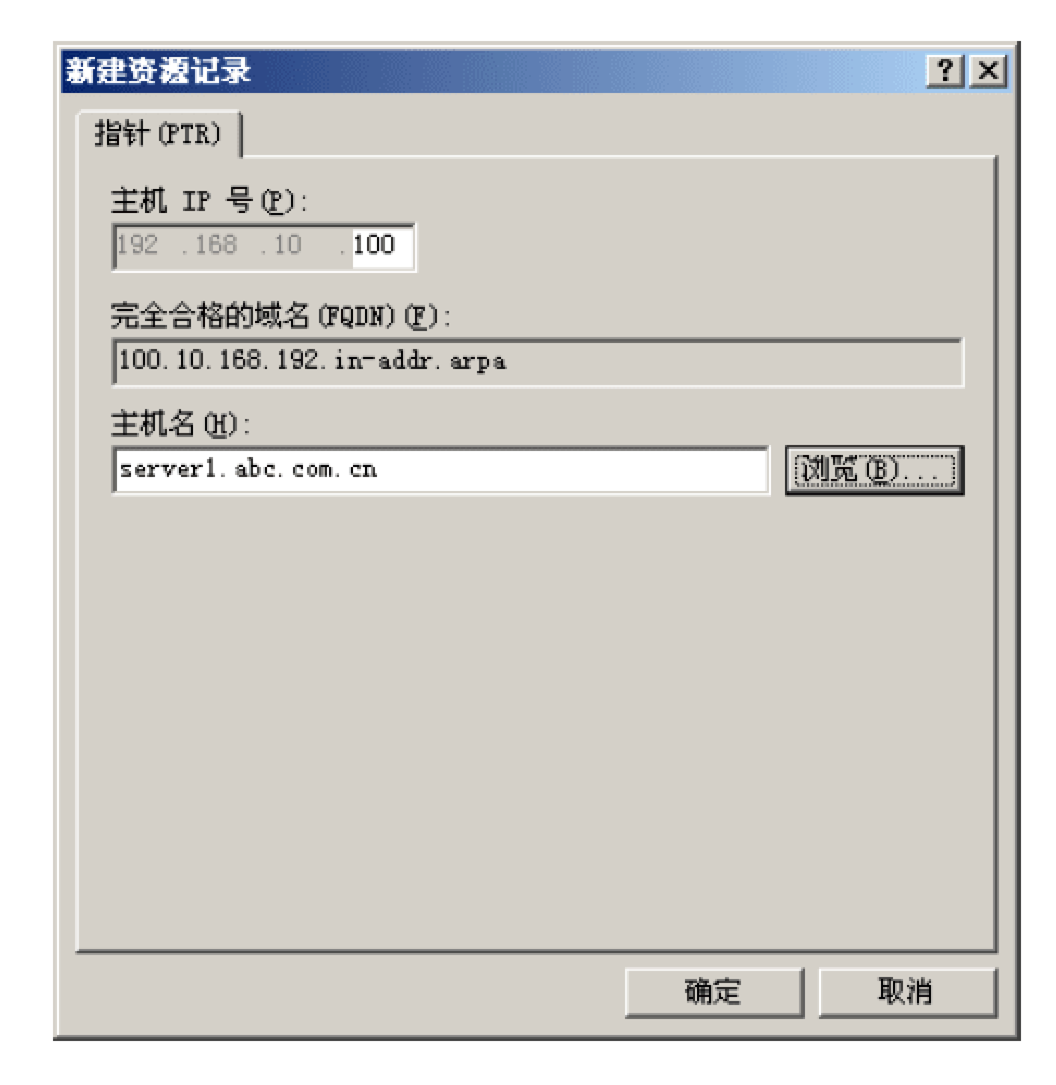


图 2-16　新建指针

2.2.1.2　Red Flag Server 下 DNS 服务器的安装与配置

1. 打开 DNS 配置工具

打开 DNS 配置工具：必须在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfdns。其启动方法有三种。

(1) 在系统主菜单中选择【系统】|【控制面板】命令，打开【控制面板】窗口，在【网络服务配置】选项卡中，双击【DNS 配置工具】选项。

(2) 在系统主菜单中选择【管理工具】|【DNS 配置工具】命令。

(3) 在运行命令或 shell 提示符下直接输入 rfdns。

2. 启动和停止 DNS 服务

启动、停止和重新启动 DNS 服务可以通过 DNS 配置工具 rfdns 来进行，也可以通过命令行终端来完成。

通过 DNS 配置工具 rfdns 来启动、停止和重新启动 DNS 服务的步骤如下。

(1) 启动 DNS 配置工具 rfdns。

(2) 在控制台菜单中选择【操作】|【所有任务】命令，然后选择【启动】命令可以启动 DNS 服务，选择【停止】命令可以停止 DNS 服务，选择【重新启动】命令可以重新启动 DNS 服务。

通过命令行终端来启动、停止和重新启动 DNS 服务的命令如下。

- 启动 DNS 服务：#/etc/init.d/named start。
- 停止 DNS 服务：#/etc/init.d/named stop。
- 重新启动 DNS 服务：#/etc/init.d/named restart。

3. 在 Red Flag Server 中添加正向查找区域

(1) 添加正向标准主要区域的步骤如下。

① 在配置工具主窗口左侧的控制台树中，单击【正向查找区域】选项。在菜单中选择【操作】|【新建区域】命令，弹出【新建区域向导】对话框，单击【下一步】按钮继续。

② 在出现的【区域类型】界面中，建立一个全新的区域。选中【主要区域】单选按钮，单击【下一步】按钮继续。

③ 在出现的【区域名称】界面中输入新建区域的名称。如果申请的是一组域名，比如 abc.com，则只要输入到二级域，而不是连同子域或主机名称一起输入，单击【下一步】按钮继续。

④ 在出现的【区域文件】界面中，如果要创建一个新的区域文件，就直接使用提示的文件名来添加数据。如果这个区域要使用从另一台计算机上复制的文件，可选中【使用此现存文件】单选按钮。选择区域文件后，单击【下一步】按钮继续。

⑤ 在出现的【正在完成新建区域向导】界面中，将显示以上步骤所设置的数据列表。如果一切设置正确，单击【完成】按钮将建立一个正向查找区域。新建的区域将添加到主窗口的控制台树中。

(2) 添加正向标准辅助区域的步骤如下。

① 添加正向标准辅助区域与添加正向标准主要区域的步骤相同，在【区域类型】界面中选中【辅助区域】单选按钮，单击【下一步】按钮继续。

② 在【区域名称】界面中为新添加的区域命名后，单击【下一步】按钮进入【设置复制区域】界面，设置想要复制区域的服务器。此步骤用来设置想要复制区域的 DNS 服务器源，可以一次复制多个服务器的数据。

③ 在【IP 地址】中输入可复制的服务器 IP 地址后单击【添加】按钮；也可以在【服务器名】文本框中输入服务器的主机名后，单击【解析】按钮获得其 IP 地址再添加。

④ 单击【下一步】按钮，然后依向导提示完成设置。新建的区域将添加到主窗口的控制台树中。

4. 在 Red Flag Server 中添加反向查找区域

这里仅介绍添加反向标准主要区域的过程。添加反向标准辅助区域的过程与添加正向标准辅助区域的过程基本相同，这里就不再介绍了。添加反向标准主要区域的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，单击【反向查找区域】选项。在菜单中选择【操作】|【新建区域】命令，弹出【新建区域向导】对话框，单击【下一步】按钮继续。

(2) 在出现的【区域类型】对话框中，开始建立一个全新的区域，选中【主要区域】单选按钮，单击【下一步】按钮继续。

(3) 在出现的【反向查找区域】界面的【网络 ID】文本中，应该以 DNS 服务器 IP 地址的前三段来设置反向查找区域。例如，我们所使用 DNS 服务器的 IP 地址是 172.16.82.11，则取其前三段即 172.16.82。然后，系统会在【反向查找区域名称】文本框中自动设置为

82.16.172.in-addr.arpa，单击【下一步】按钮继续。

(4) 在出现的【区域文件】界面中，直接使用默认的文件名即可，单击【下一步】按钮继续。

(5) 在出现的【正在完成新建区域向导】界面中，将显示以上步骤所设置的数据列表。如果一切设置正确，单击【完成】按钮将建立一个反向查找区域。新建的区域将添加到主窗口的控制台树中。

5. 在 Red Flag Server 中配置区域属性

1) 修改区域的起始授权机构(SOA)记录

SOA(Start of Authority)用来识别域名中由哪一个名称服务器负责信息授权，在区域数据库文件中，第一条记录必须是 SOA 的设置记录。

在配置工具主窗口左侧的控制台树中，选择相应的区域。选择菜单中的【操作】|【属性】命令，或右击选择快捷菜单中的【属性】命令，打开【区域属性】对话框，切换到【起始授权机构(SOA)】选项卡。

如有需要，可以修改起始授权机构(SOA)的属性。要调整【刷新间隔】、【重试间隔】或【过期间隔】，在下拉列表中选择以秒、分钟、小时、天或星期为单位的时间段，然后在文本框中输入数字。单击【应用】按钮，保存调整后的间隔。完成更改后单击【确定】按钮使修改生效。

2) 将其他 DNS 服务器指定为区域的权威服务器

在配置工具主窗口左侧的控制台树中选择相应的区域。选择菜单中的【操作】|【属性】命令，或右击选择快捷菜单中的【属性】命令，打开【区域属性】对话框，切换到【名称服务器】选项卡。

如果要向列表中添加名称服务器，单击【添加】按钮，即可弹出【新建名称服务器】对话框。按 IP 地址指定其他的 DNS 服务器，然后单击【添加】按钮将它们加入列表。也可以通过指定服务器 IP 地址或输入其 DNS 名称将区域添加到权威服务器的列表中。输入名称时，单击【解析】按钮可以在将它添加到列表之前将其名称解析为 IP 地址。

使用该过程指定的 DNS 服务器将被加入到该区域的现有名称服务器(NS)资源记录中。

3) 为辅助区域更新主控服务器

在配置工具主窗口左侧的控制台树中，选择相应的辅助区域。选择菜单中的【操作】|【属性】命令，也可以右击选择快捷菜单中的【属性】命令，打开【区域属性】对话框。

切换到【常规】选项卡，在【IP 地址】中，为新的主控服务器指定 IP 地址并单击【添加】以便在列表中更新。

6. 管理资源记录

1) 添加主机资源记录

向区域中添加主机资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的【操作】|【新建主机】命令，或右击选择快捷菜单中的【新建主机】命令，打开【新建主机】对话框。

(2) 在【名称】文本框中，输入新增主机记录的名称。不需要填上整个域名，比如要

新增 sales 名称，只需输入 sales，而不是 sales.abc.com。

(3) 在【IP 地址】文本框中，输入新建主机的实际 IP 地址。

(4) 单击【添加主机】按钮，新增的主机记录将显示在主窗口右侧的列表中。重复上述操作可以向区域中添加多个主机资源记录。

2) 添加别名(CNAME)的资源记录

设置别名可以让一个主机拥有多个主机名称。例如，一个主机当作为 Web 服务器时为 www.abc.com，而当作为 FTP 服务器时可以是 ftp.abc.com。向区域添加别名(CNAME)的资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的【操作】|【新建别名】命令，或右击选择快捷菜单中的【新建别名】命令，打开【新建资源记录】对话框。

(2) 在【别名】文本框中，输入别名。在【目标主机的完全合格的域名】文本框中，输入使用此别名的 DNS 主机的完全合格域名。

(3) 单击【确定】按钮，完成新增主机别名的操作。新增的主机别名将出现在主窗口右侧的列表中。

3) 添加邮件交换器资源记录

向区域添加邮件交换器(MX)资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的【操作】|【新建邮件交换器】命令，或右击选择快捷菜单中的【新建邮件交换器】命令，打开【新建资源记录】对话框。

(2) 切换到【邮件交换器】选项卡。在【主机或子域】文本框中，输入使用此记录发送邮件的服务器域名。在【邮件服务器的完全合格的域名】文本框中，输入邮件交换器或邮件服务器主机(发送指定域名的邮件)的 DNS 主机名。

(3) 若该区域内有多台同样域名的邮件服务器，可以调整此区域的【邮件服务器优先级】，数字较小的优先级较高。

(4) 单击【确定】按钮，完成新增邮件交换器的操作。新增的邮件交换器记录将显示在主窗口右侧的列表中。

4) 添加指针(PTR)资源记录

向反向查找区域添加指针(PTR)资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择适当的反向查找区域。选择菜单中的【操作】|【新建指针】命令，或右击选择快捷菜单中的【新建指针】命令，弹出【新建资源记录】对话框。

(2) 在【主机 IP 号】文本框中，输入主机 IP 地址的 8 位字节数。在【主机名】文本框中，输入 DNS 主机的完全合格域名，该计算机使用此指针记录提供反向搜索(把 IP 地址解析为域名)。

(3) 单击【确定】按钮，建立新增的指针。新增的指针记录将显示在主窗口右侧的列表中。

5) 修改区域中的现有资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域，窗口右侧会显示该区域的详

细信息列表。选择要修改的资源记录项，选择菜单中的【操作】|【属性】命令，或右击选择快捷菜单中的【属性】命令，打开【区域属性】对话框。在相应的属性对话框中，可以根据需要查看或编辑任何可以修改的属性。

6)　从区域中删除资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域，窗口右侧会显示该区域的详细信息列表。选中要删除的资源记录项，选择菜单中的【操作】|【删除】命令，或右击该项，并在快捷菜单中选择【删除】命令。当出现提示对话框时，确认是否删除所选的资源记录即可。

7)　使用 rfdns 编辑器

为了使用户能够全面地配置 DNS 服务器支持的全部功能，rfdns 配置工具中提供了一个配置文件编辑器。用户可以通过它直接对 DNS 配置文件进行手工修改(后面将要详细介绍)。在菜单中选择【查看】|【编辑器】命令，可以切换文件编辑窗口的隐藏与显示。

选中某一区域或资源记录，其对应的配置内容会在配置文件编辑器中被高亮显示出来。对相应配置文件进行编辑后，单击工具栏中的【存储配置文件】按钮。

配置工具也可以检查配置文件的语法错误，检查结果会显示在消息窗口中。如果出现语法错误，应根据提示进行修改。在开始手工修改配置文件后，不要在存储之前使用配置工具提供的其他配置功能，否则所作的修改将会被覆盖。配置文件修改并存储后，必须重新启动 DNS 服务器才能使修改生效。

2.2.1.3　Linux 操作系统下的 DNS 客户端配置文件

每一台 Linux 主机要实现域名解析(不管它是不是域名服务器)都需要配置 DNS 客户端配置文件。Linux 操作系统下的 DNS 客户端配置文件主要有两个：一个是名称转换控制文件，另一个是域名转换程序配置文件。

1.　名称转换控制文件

不同的 Linux 中使用不同的名称转换控制文件，在 Red Flag Linux 中使用/etc/nsswitch.conf 文件，而在 Red Hat Linux 中，使用/etc/host.conf 文件。

在 Red Flag Linux 中，/etc/nsswitch.conf 文件用于存放本机主机名以及经常访问 IP 地址的主机名。和域名服务有关的一项是 hosts。在对 IP 进行域名解析时，可以设定为先访问该文件，再访问 DNS，最后访问 NIS。这一行文件内容如下：

```
hosts: files dns nisplus nis
```

在 Red Hat Linux 中，/etc/host.conf 文件是用来控制转换程序的设置文件。该文件告诉转换程序使用哪些服务及按照什么顺序进行。可以通过 order 来指定，这一行文件内容如下：

```
order hosts,dns,nis
```

在 Red Hat Linux 中，使用/etc/hosts 文件来存放本机主机名以及经常访问 IP 地址的主机名。

2.　域名转换程序配置文件

该配置文件是/etc/resolv.conf，它用来设置主机所在域名、域名查找的顺序以及域名服

务器的 IP 地址。下面是一个域名转换程序配置文件的例子：

```
domain abc.com.cn
search abc.com.cn xyz.com.cn
nameserver 10.1.14.61
nameserver 10.1.14.62
```

【说明】

- domain 用来定义主机的本地域名。
- search 用来设置查找域名表。如果要查询的只有主机名称，而不含完整的域名时，会加上这里的域名去查找。如果没设置，就会自动加上 domain 设置的域名。
- nameserver 列出域名服务器的 IP 地址。可以设置多个域名服务器，若第一个不能提供服务时就会自动使用第二个。如果 Linux 主机本身就是一台域名服务器，为提高查询速度，应把第一个 nameserver 设置为本地环回地址 127.0.0.1。

2.2.1.4 Linux 操作系统下的 DNS 服务器配置文件

在 Linux 操作系统下，有一些和 DNS 服务器配置密切相关的文件，这里作一下简要介绍。下面以一个组织的主域名服务器配置为例。该组织的域名为 abc.com.cn，所使用的网络地址为 210.45.12.0，共有两台服务器：一台的 IP 地址是 210.45.12.100，名字是 a100，它用作域名服务、电子邮件服务；另一台的 IP 地址是 210.45.12.101，名字是 a101，它用作 Web 服务。

1. DNS 服务主配置文件/etc/named.conf

该文件是域名服务器守护进程 named 启动时读取到内存的第一个文件。在该文件中定义了域名服务器的类型、所授权管理的域以及相应数据库文件和其所在的目录。该文件默认的名字是/etc/named.conf。

named.conf 文件的配置一般包括一个全局配置选项(options)部分和多个区(zone)声明部分。

1) 全局配置选项 options

最常用的全局配置选项是定义服务器配置文件的工作目录和转发服务器的 IP 地址。例如：

```
options {
directory "/var/named";
forwarders{
    202.96.134.133;
        };
};
```

【说明】

- directory 指定了 DNS 数据文件的存放目录是/var/named。
- forwarders {202.96.134.133;}，其中 202.96.134.133 是转发 DNS 服务器的地址，forwarders 参数指定其后的 IP 所在的服务器作为备选的 DNS 服务器。也就是说，把本机 DNS 不能解析的主机发送到这个备选的 DNS 服务器上，让它来进行解析。

2)　区声明

区声明是配置文件中最重要的部分，可有多个区声明，每一条区声明需要说明域名、服务器的类型和域信息源三项。例如：

```
zone "abc.com.cn" IN {
type master;
file " named.hosts";
notify no;
};
```

【说明】

- zone " abc.com.cn " 用于定义这个区的名称。
- type 指定服务器类型。可选的类型有 master、slave 和 hint。master 说明一个区的主域名服务器；slave 说明一个区的辅助域名服务器；hint 说明一个区的高速缓存文件。可以通过该参数来说明这台服务器是主域名服务器、辅助域名服务器或缓存域名服务器。
- file 指明该区资源记录存放的文件名称。
- notify 用来设置是否自动发出 DNS NOTIFY 信息，其预设值为 yes，也就是当主域名服务器中数据库文件发生修改时，自动发出 DNS NOTIFY 信息，当辅助域名服务器收到这个信息后就自动向主域名服务器确认是否需要更新资料，并自动更新。

(1)　根域名区声明

该区用来告诉域名服务器的守护程序必须维护一个高速缓存域名服务器，同时还告诉域名服务器的守护程序利用什么文件去初始化高速缓存，其类型必须设置为 hint，该文件一般存放在 named.ca 中。例如：

```
zone "." IN {
type hint;
file "named.ca";
};
```

(2)　反向环回地址区声明

反向环回地址区主要用于设置环回地址反向解析文件的位置。其内容如下：

```
zone "0.0.127.in-addr.arpa" IN {
type master;
file "named.local";
allow-update { none; };
};
```

(3)　正向域名解析区声明

正向域名解析区主要用来设置本区域正向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器，则不需要配置该区；若该 DNS 服务器是一个主域名服务器，则 type 指定为 master。下面的例子是一个主域名服务器，其域名为 abc.com.cn，正向域名解析数据存放在 named.hosts 文件之中。

```
zone " abc.com.cn " IN {
```

```
type master;
file " named.hosts";
allow-update { none; };
};
```

如果是辅助域名服务器，则 type 指定为 slave，同时还要指定主域名服务器的 IP 地址，以便进行数据库更新。其格式为 masters{<主域名服务器的 IP 地址>}。例如，主域名服务器地址为 210.45.12.101，则其内容如下：

```
zone " abc.com.cn " IN {
type slave;
file "named.hosts";
masters{210.45.12.101}
};
```

(4) 反向域名解析区声明

反向域名解析区主要用来设置本区域反向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器，也不需要配置该区；若该 DNS 服务器是一个主域名服务器，则 type 指定为 master。下面的例子是一个主域名服务器，它负责 210.45.12.0 网络的反向解析，反向域名解析数据存放在 named.rev 文件中。

```
zone "12.45.210.in-addr.arpa" IN {
type master;
file "named.rev";
allow-update { none; };
};
```

如果是辅助域名服务器，则 type 指定为 slave，同时还要指定主域名服务器的 IP 地址，以便进行数据库更新。其格式为 masters{<主域名服务器的 IP 地址>}。例如，主域名服务器地址为 210.45.12.101，则内容如下：

```
zone "12.45.210.in-addr.arpa" IN {
type slave;
file "named.rev";
masters{210.45.12.101}
};
```

2. DNS 的数据库文件和资源记录

1) 资源记录

在/etc/named.conf 文件中所定义的文件都是 DNS 数据库文件(如本例中 named.ca、named.local、named.hosts、named.rev)，每个文件都由资源记录构成。每条资源记录包含与特定主机的有关信息。而每一条资源记录通常包含 5 项，按一行记录在文本文件之中，其格式如下：

```
[域名] [存活期 ttl] IN <记录类型> <记录数据>
```

- 域名：给出要定义的资源的域名，该域名通常用来作为域名查询时的关键字。
- 存活期：在存活期内，该记录有效；存活期过后，该记录不再有效。

- IN：将记录标识为一个 Internet DNS 资源记录。
- 记录类型：该项表明资源记录的类型(下面将详细介绍)。
- 记录数据：说明和该资源记录相关的信息，通常由资源记录类型来决定。

资源记录主要有以下几种类型。

- 主机(A)记录：用来记录在正向查找区域内的主机及其 IP 地址。用户可通过该类型的资源记录把主机域名映射为 IP 地址。
- 主机别名(CNAME)记录：在某些情况下，需要为区域内的一台主机创建多个主机名称。例如，一台主机同时是 Web 服务器与 FTP 服务器，则可以为该主机取两个不同名称，当作为 Web 服务器时域名是 www.abc.com，而当作为 FTP 服务器时域名可以是 ftp.abc.com。
- 邮件交换器(MX)记录：当用户将邮件送到本地邮件服务器后，本地邮件服务器必须将邮件送到目的地邮件服务器，而目的地的邮件服务器 IP 地址可以向 DNS 服务器查询。邮件交换器记录就是指定哪些主机负责接收该区域的电子邮件，如果在此区域内创建了多个邮件交换器记录，可以调整此区域邮件服务器的优先级，数字较低的优先级较高。
- 指针(PTR)资源记录：用来记录在反向查找区域内的 IP 地址及主机。用户可通过该类型的资源记录把 IP 地址映射为主机域名。
- 起始授权机构(SOA)记录：用来记录此区域中的主要名称服务器以及管理此 DNS 服务器的管理员的电子邮件信箱。
- 名称服务器(NS)记录：用来记录管辖此区域的名称服务器，包括主域名服务器和辅助域名服务器。

2)　高速缓存初始化文件

在 Linux 系统上，通常在/var/named 目录下已经提供了一个 named.ca。该文件中包含了 Internet 的顶层域名服务器，但这个文件通常会有变化，所以建议最好从 Inter NIC(Internet 网络信息中心)下载最新的版本。该文件可以通过匿名 ftp 下载。

3)　环回地址转换文件

该文件用来说明“环回地址”的 IP 地址到主机名的映射。其文件名由/etc/named.conf 中反向环回地址区定义，通常为/var/named/named.local。该文件的内容如下：

```
$TTL  86400
@       IN   SOA     localhost.  root. localhost. (
                         2001110600 ;    serial
                         28800       ;refresh
                         14400       ;retry
                         3600000     ;expire
                         86400 )     ;minimum
        IN   NS      localhost.
1       IN   PTR     localhost.
```

【说明】

- 此文件的内容是特定的，在不同的域的域名服务器上，所要修改的只是 SOA 记录和 NS 记录。

- PTR 记录的最后域名为完全标识域名，以“.”结束。

4) 正向域名转换数据文件

该文件指定了域中主机域名同 IP 地址的映射，实现域名的正向解析。其文件名由/etc/named.conf 中正向域名解析区声明定义，本例中该文件名为/var/named/named.hosts。其内容如下：

```
$TTL  86400
@       IN   SOA     a100.abc.com.cn.   root.abc.com.cn. (
                     2001110600 ; serial
                     28800 ; refresh
             14400 ; retry
             3600000 ; expire
             86400 ; minimum
             )
             IN  NS   a100.abc.com.cn.
             IN  MX   10  a100.abc.com.cn.
localhost.   IN  A    127.0.0.1
a100         IN  A    210.45.12.100
a101         IN  A    210.45.12.101
www          IN  CNAME   a101
```

【说明】

- 在文件中所有的记录行都要顶格写，前面不能有空格。
- 行 IN　NS　a100.abc.com.cn.说明该域的域名服务器，至少应该定义一个。
- 行 IN　MX　10　a100.abc.com.cn.是一条邮件交换器(MX)记录，指明了单位的邮件交换器是 a100.abc.com.cn，它负责处理邮件地址的主机部分为@abc.com.cn 的邮件，10 表示优先级别。
- 类似于行 a100 IN A 210.45.12.100 的是一系列的 A 记录，表示主机名和 IP 地址的对应关系。a100 是主机名，210.45.12.100 是它的 IP 地址。
- 行 www IN CNAME a101 表示一条定义别名的记录。即 www.abc.com.cn 和 a101.abc.com.cn 表示同一台主机。

5) 反向域名转换数据文件

该文件主要定义了 IP 地址到主机名的转换，实现域名的反向解析。IP 地址到主机名的转换是非常重要的，Internet 上的很多应用，如 NFS、Web 服务等都要用到该功能。其文件名由/etc/named.conf 中反向域名解析区声明定义，本例中其名称为/var/named/named.rev。该文件的内容如下：

```
$TTL  86400
@       IN   SOA     a100. abc.com.cn.   root. abc.com.cn. (
             2001110600 ; serial
             28800 ; refresh
             14400 ; retry
             3600000 ; expire
             86400 ; minimum
             )
```

```
        IN   NS      abc.com.cn.
100     IN   PTR     a100.abc.com.cn.
101     IN   PTR     a101.abc.com.cn.
```

【说明】

- PTR 记录用于定义 IP 地址名到主机域名的映射。即 IP 地址 210.45.12.100 对应的主机名为 a100.abc.com.cn，IP 地址 210.45.12.101 对应的主机名为 a101.abc.com.cn。
- PTR 记录的最后一项必须是一个完整的标识域名，以“.”结束。

注意：在辅助域名服务器和缓存域名服务器中，不需要配置正向域名转换数据文件/var/named/named.hosts 和反向域名转换数据文件/var/named/named.rev。但在辅助域名服务器中，若不存在这两个文件，域名服务器的守护程序将自动从主域名服务器中下载这两个文件，文件内容与主域名服务器完全相同；若文件存在，则检查主域名服务器中的数据是否不同于本地文件，若有变化，就下载并更新本地文件的内容；若无变化，就加载本地磁盘文件，不必从远程下载。

3. 启动、停止和重新启动域名服务器

默认安装时，域名服务器的守护程序为/etc/rc.d/init.d/named，是域名服务的最主要文件。用户可以通过该程序启动、重新启动、停止域名服务。其命令分别是：

```
#/etc/rc.d/init.d/named start
#/etc/rc.d/init.d/named restart
#/etc/rc.d/init.d/named stop
```

如果设定 DNS 服务在计算机启动时自动启动或不启动，可以通过 chkconfig 命令来设定。该命令格式为

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如，我们希望计算机在运行级别 3、5 的情形下启动时自动启动 DNS 服务，则命令为

```
#chkconfig --level 35 named on
```

再如，我们希望计算机在运行级别 2 的情形下启动时不启动 DNS 服务，则命令为

```
#chkconfig --level 2 named off
```

2.2.2 典型例题分析

例 1　阅读以下关于 Linux 系统中域名系统(DNS)的说明，回答问题 1～问题 4。(2009 年 5 月下午试题一)

【说明】

DNS 是一种 TCP/IP 的标准服务，负责 IP 地址和域名之间的转换。在 Linux 系统中，DNS 可以由 BIND(Berkeley Internet Names Domain)软件来实现。

【问题 1】(每空 1.5 分，共 6 分)

请在(1)～(4)空白处填写适当的内容。

DNS 服务器可以管理一个域，也可以管理多个域，域名服务器可以分为转发域名服务器、缓存域名服务器__(1)__和__(2)__等类型。将域名转换为 IP 地址的过程称为__(3)__，将 IP 地址转换为域名的过程称为__(4)__。

【问题 2】(每空 2 分，共 4 分)

请选择适当的内容填写在(5)、(6)空白处。

管理员可以在命令行终端下，通过__(5)__命令启动 DNS 服务；通过__(6)__命令停止 DNS 服务。

A. /etc/init.d/named start　　B. ./etc/init.d/dns up

C. ./etc/init.d/named stop　　D. ./etc/init.d/dns down

【问题 3】(每空 1 分，共 3 分)

请在(7)～(9)处填写恰当的内容。

在 Linux 系统中配置域名服务器，该服务器上文件 named.conf 的部分内容如下：

```
Options {
        directory '/var/named';
   };
   zone '.' {
       type hint;
       file 'named.ca';
   }
   zone 'localhost' IN{
        file 'localhost.zone'
        allow-update{none;};
   };
   zone '0.0.127.in-addr.arpa'{
        type master;
        file 'named.local';
   };
   zone 'test.com'{
        type (7) ;
        file 'test.com';
   };
   zone '40.35.222.in-addr.arpa'{
        type master;
        file '40.35.222';
            };
            Include "/etc/mdc.key";
```

填写文件中空(7)处缺少的内容。

该服务器是域 test.com 的主域名服务器，该域对应的网络地址是__(8)__，正向域名转换数据文件存放在__(9)__目录中。

【问题 4】(2 分)

某企业内部网的 DNS 服务器发生故障，如不改变客户机原有设置，该网用户是否可以

访问网络上的资源？如果可以，需要什么条件？如果不可以，试说明原因。

分析：

【问题 1】

DNS(域名系统)负责 IP 地址和域名之间的转换：将域名转换为 IP 地址的过程称为正向解析，将 IP 地址解析转换为域名的过程称为反向解析。域名服务器负责控制本地数据库中的名字解析，按照功能可划分为主域名服务器、辅助域名服务器、缓存域名服务器和转发域名服务器。主域名服务器负责维护某个区域的所有域名信息，是特定域所有信息的权威信息源；辅助域名服务器是当主域名服务器关闭、出现故障或负载过重时，作为备份服务器提供域名解析；缓存域名服务器专门用来缓存查询的地址，也可以回答查询，但没有授权；转发域名服务器负责所有非本地域名的本地查询。

【问题 2】

DNS 服务的启动和停止可以在控制台中进行控制，也可以在命令行终端下实现。在命令行终端下可通过命令/etc/init.d/named start 和/etc/init.d/named stop 完成。

【问题 3】

named.conf 文件是主域名服务器的主配置文件。

首先设定 named.conf 的 options 部分，这里规定了 DNS 服务器的权限。目录(Directory)选项允许指定名字服务器的工作目录路径，这里为/var/named。全部域或区域文件都保存在服务器的工作目录中。

然后设置管理域内如何作正向解析和反向解析，使用关键字 zone 定义区域。需要两个 zone 结构，一个用于正向解析，另一个用于反向解析。

```
zone 'test.com'{
    type master;
    file 'test.com';
};
```

这个 zone 用于正向解析。其中，type 是该 zone 的类型，DNS 服务器一共规定了 3 种类型的 zone：master、slave 和 hint。最上层的 DNS 服务器用 hint 类型，DNS 主服务器使用 master 类型，从服务器使用 slave 类型。该服务器是域 test.com 的主域名服务器，类型为 master。file 设置了正向解析数据库文件的相对路径。

该 zone 把名字服务器设置为 test.tom 域“主要”的授权名字服务器，所有对 test.tom 的主机名到 IP 的转换都由该名字服务器处理，并且转发区域配置信息和资源记录在 test.com 文件中保存。

```
zone '40.35.222.in-addr.arpa'{
    type master;
    file '40.35.222';
}
```

这个 zone 用于反向解析，反向解析的 zone 必须设置 IP 段。这里将 IP 段设为 222.35.40 的意思是反向适用于 222.35.40.*这个范围内的 IP 地址。该 zone 语句把名字服务器设置为 222.35.40.0 网络的“主要”名字服务器，所有对该网络的 IP 地址到主机名的转换都由该名字服务器处理，反向 DNS 配置信息和资源记录保存在 40.35.222 文件中。

【问题 4】

用户访问网络实际上是使用 IP 地址来完成的，但 IP 地址不易记住，才出现了域名。用户使用域名访问网络时，首选要通过 DNS 服务器进行域名解析，获得该网络的 IP 地址，然后才能访问网络。若 DNS 服务器发生故障，只要用户知道被访问端的 IP 地址，则可直接使用该地址访问网络上的资源，无须通过 DNS 服务器进行域名解析。

答案：

【问题 1】

(1) 主域名服务器

(2) 辅助域名服务器

(3) 正向解析　　　(4) 反向解析

注：(1)和(2)的答案可以互换。

【问题 2】

(5) A　(6) C

【问题 3】

(7) master　(8) 222.35.40.0　(9) /var/named

【问题 4】

可以，需要知道被访问端的 IP 地址。

例 2　阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2007 年 11 月下午试题二)

【说明】

某服务器既是 Web 站点又是 FTP 服务器，Web 站点的域名为 www.test.com，Web 站点的部分配置信息如图 2-17 所示，FTP 服务器的域名为 ftp.test.com。



图 2-17　某服务器的 Web 站点部分配置信息

Windows Server 2003 系统中可通过【管理您的服务器】向导来配置 DNS。在 DNS 服务器中为 Web 站点添加记录时，新建区域名称如图 2-18 所示。

【问题 1】(2 分)

区域文件界面如图 2-19 所示，默认情况下区域文件名为__(1)__。

A．test.com.dns　B. test.com.www　C. test.com.ftp　D. test.com

【问题 2】(4 分)

区域建成后，右击区域名称，在如图 2-20 所示的下拉菜单中选择【新建主机】命令，在图 2-21 中为 www.test.com 建立正向搜索区域记录，名称栏应填入__(2)__，IP 地址栏应填入__(3)__。

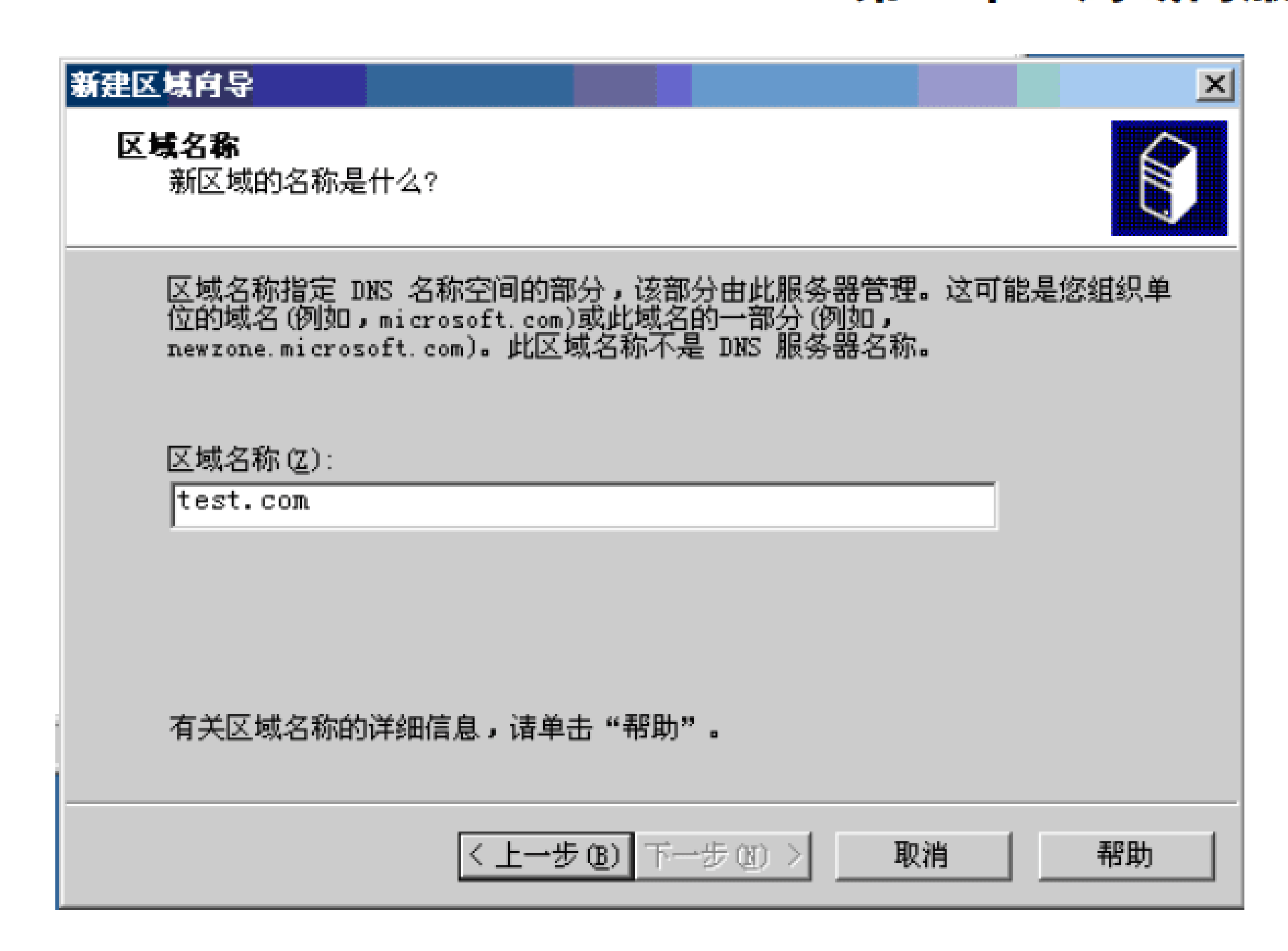


图 2-18　【新建区域向导】对话框(一)

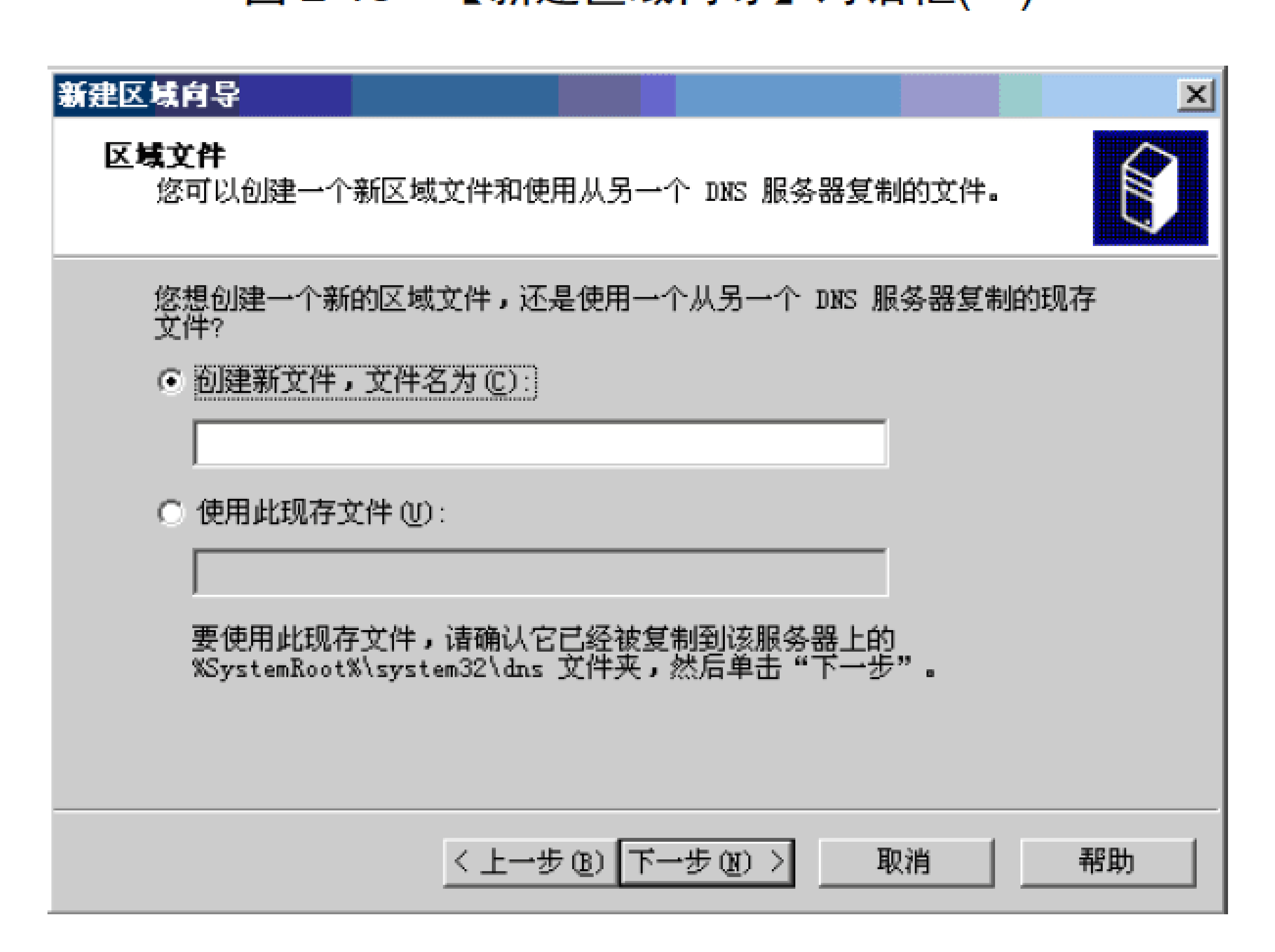


图 2-19　【新建区域向导】对话框(二)



图 2-20　下拉菜单

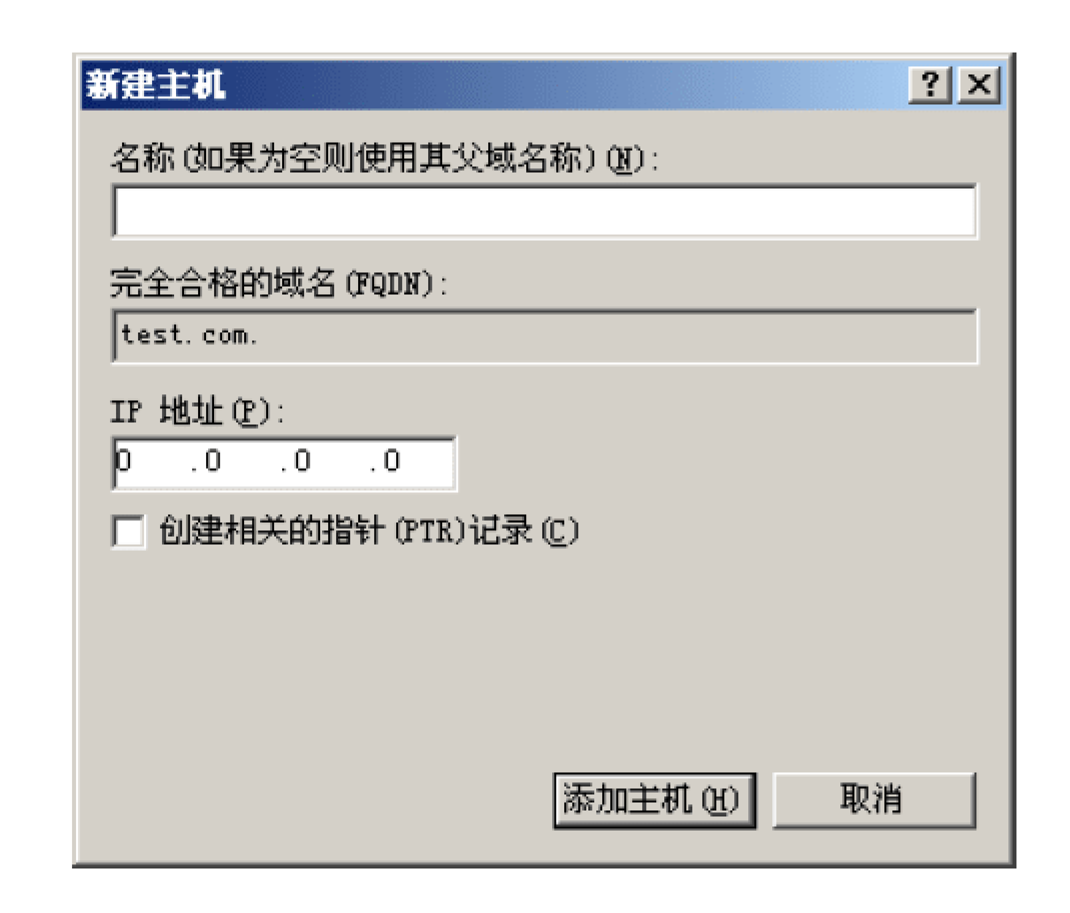


图 2-21　【新建主机】对话框

【问题 3】(2 分)

在如图 2-20 所示的下拉菜单中选择__(4)__命令，可为 ftp.test.com 建立正向搜索区域

记录。

A．【新建邮件交换器】　　B．【新建域】　　C．【新建别名】

【问题 4】(5 分)

该 DNS 服务器配置的记录如图 2-22 所示。

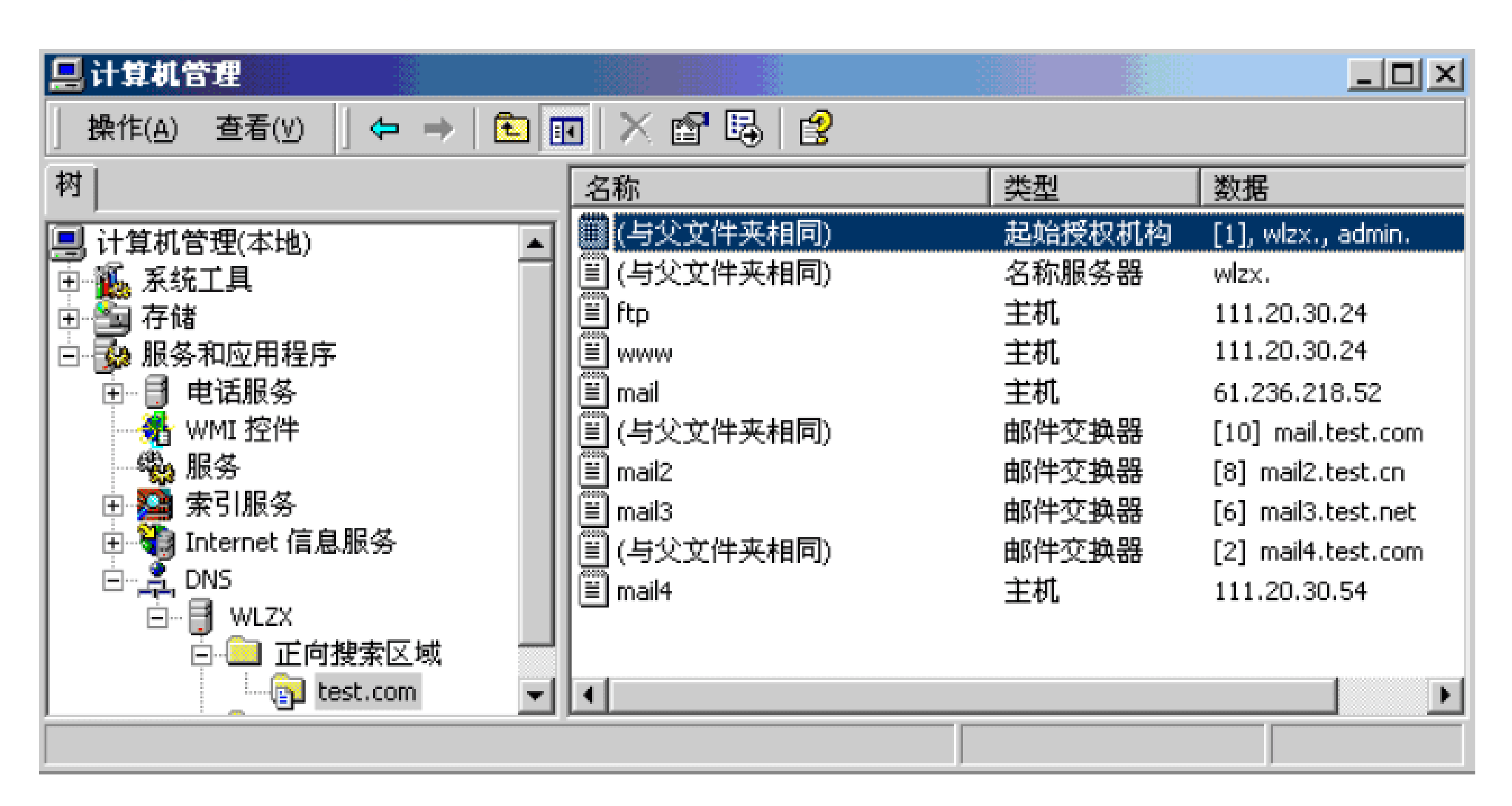


图 2-22 【计算机管理】窗口

邮件交换器中优先级别最高的是__(5)__。(3 分)

A．[10]mail.test.com　　B．[8]mail2.test.cn

C．[6]mail3.test.net　　D．[2]mail4.test.com

在浏览器的地址栏中输入__(6)__，可以访问该 Web 服务器的默认 Web 站点。(2 分)

A．http://www.test.com　　B．http://www.test.net

C．http://www.test.com:8080　　D．http://www.test.net:80

【问题 5】(2 分)

在客户端可以通过__(7)__来测试 DNS 是否配置成功。

A．ping www.test.com　　B．ping 110.20.30.24

C．ping test.com　　D．ping 110.20.30.54

分析：本例题考查的是 DNS 服务器的配置情况。

【问题 1】

默认情况下区域文件名为“区域名+.dns”，故选 A。

【问题 2】

在区域建成后，www.test.com 的 www 即为正向搜索区域记录的名称，故名称栏应填入 www；IP 地址栏是域名 www.test.com 对应的 IP 地址，故应填入 111.20.30.24。

【问题 3】

要为 ftp.test.com 建立正向搜索区域记录，由于区域 test.com 已经存在，可采用新建主机或新建别名创建记录，故选 C。

【问题 4】

4 个选项中，方括号内是各个选项的优先级，故 A、B、C、D 的优先级分别是 10、8、6、2，数字越小优先级越高，故优先级最高的是[2]mail4.test.com。图 2-17 中已经显示了 Web 服务器的默认端口为 8080，故 http://www.test.com:8080 可以访问该 Web 服务器的默认

Web 站点。

【问题 5】

考查 ping 命令的使用。ping www.test.com 需要将域名转换成 IP 地址，然后再测试到 110.20.30.24 的连通性；ping 110.20.30.24 只能说明和主机的连接是连通的，因为它不需要进行域名的转换；ping 针对具体主机，ping test.com 不可达；ping 110.20.30.54 是检查到邮件主机的连通性。

答案：

【问题 1】

(1)　A

【问题 2】

(2)　www　　　(3)　111.20.30.24

【问题 3】

(4)　C

【问题 4】

(5)　D

(6)　C

【问题 5】

(7)　A

2.2.3　同步练习

1．阅读以下说明，回答问题 1～问题 5，将解答填入对应的答案栏内。

【说明】

某公司在国际网络互联中心申请了一个 C 类的 IP 地址 210.45.12.0/24，域名为 abc.com.cn。该公司有一台该 Web 服务器(IP 地址为 210.45.12.11，主机名为 S1)、一台 FTP 服务器(IP 地址为 210.45.12.12，主机名为 S2)、一台 MAIL 服务器(IP 地址为 210.45.12.13，主机名为 S3)和一台 DNS 服务器(IP 地址为 210.45.12.14，主机名为 S4)。若你是该公司的网络管理员，使用一台装有 Windows Server 2003 的服务器作为 DNS 服务器。

【问题 1】该服务器必须是什么类型的 DNS 服务器？

【问题 2】该 DNS 服务器的正向查找区域是什么？反向查找区域是什么？

【问题 3】现已在正向查找区域中添加了一些主机记录，当用户的浏览器地址栏中输入 http://s1.abc.com.cn 时可以访问该公司的主页，但输入 http://www.abc.com.cn 时却不能访问该公司的主页，问题出在哪儿？如何解决？

【问题 4】原来该公司用户的电子邮件地址格式是 xxx@mail.abc.com.cn，现在想把它改为 xxx@abc.com.cn。除了在邮件服务器上作修改之外，在域名服务器上还要做哪些修改？

【问题 5】现在反向查找区域添加了一个指针(PTR)记录，该记录的作用是什么？

2．回答问题 1～问题 3，将解答填入对应的答案栏内。

【问题 1】DNS 的作用是什么？

【问题 2】Internet 中的域名是如何组织的?

【问题 3】Internet 域名解析有哪两种方式?

2.2.4　同步练习参考答案

1.

【问题 1】主域名服务器。

【问题 2】abc.com.cn、12.45.210.in-addr.arpa。

【问题 3】可能是没有将 s1.abc.com.cn 的别名设置为 www.abc.com.cn，或者设置不正确。可以在正向查找区域中增加一条别名(CNAME)记录，使真实主机名为 s1.abc.com.cn，别名为 www.abc.com.cn。

【问题 4】在正向查找区域中，删除原有的邮件交换器记录(MX)，新建一条邮件交换器记录(MX)，在【主机或域名】处不要填写任何内容，服务器地址设置为 s3.abc.com.cn。

【问题 5】实现 IP 地址向域名的映射。

2.

【问题 1】DNS 的作用是将符号化的域名映射为 IP 地址。

【问题 2】Internet 中的域名是按树形结构组织的。

【问题 3】Internet 域名解析有递归解析和迭代解析两种方式。

2.3　电子邮件服务

2.3.1　考点辅导

2.3.1.1　Windows Server 2003 下电子邮件服务器的安装与配置

我们可以通过 Windows Server 2003 提供的 POP3 服务和 SMTP 服务架设小型邮件服务器来满足需要。

1. 电子邮件服务器的安装

其具体安装步骤如下。

(1) 选择【开始】|【管理工具】|【管理您的服务器】命令，出现服务器管理窗口。单击【添加或删除角色】链接，单击【下一步】按钮，系统显示【服务器角色】界面，选中【邮件服务器(POP3，SMTP)】选项，如图 2-23 所示。

(2) 单击【下一步】按钮，弹出【配置 POP3 服务】界面，其中包括选择身份验证方法和输入电子邮件域名两部分。身份验证方法包括本地 Windows 帐户身份验证和加密密码文件两种验证方式。选择身份验证方式、输入电子邮件域名，如图 2-24 所示。

(3) 单击【下一步】按钮，显示【选择总结】界面，如图 2-25 所示。

(4) 确认选择后，单击【下一步】按钮，按照系统提示插入光盘，如图 2-26 所示。

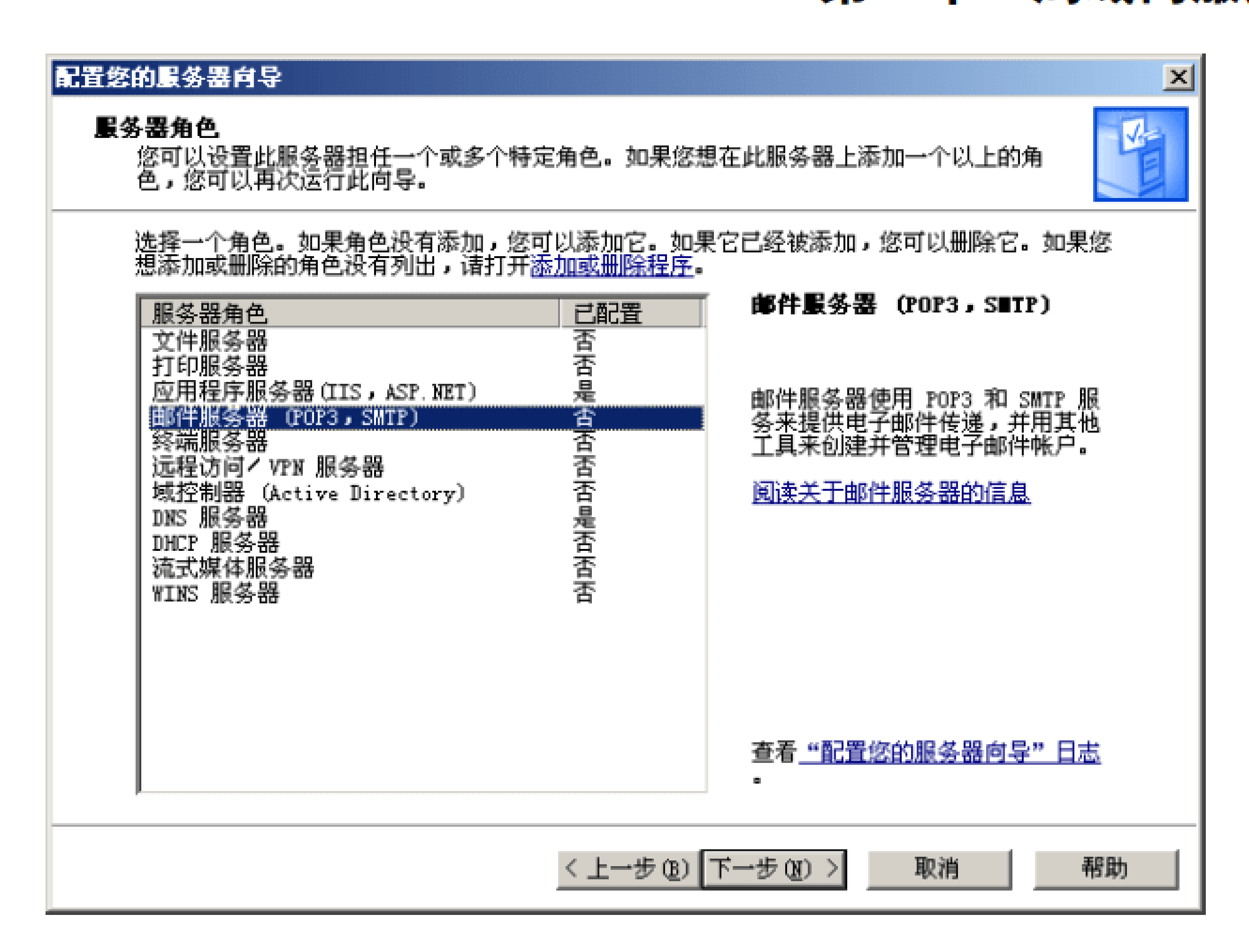


图 2-23　【服务器角色】界面



图 2-24　【配置 POP3 服务】界面



图 2-25　【选择总结】界面

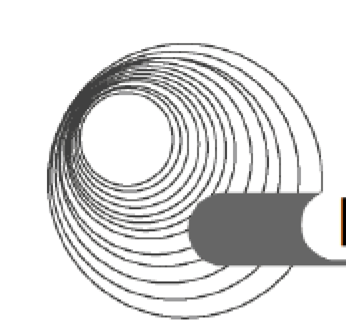




图 2-26 【插入磁盘】对话框

(5) 系统自动进行电子邮件服务组件的安装，如图 2-27 所示。

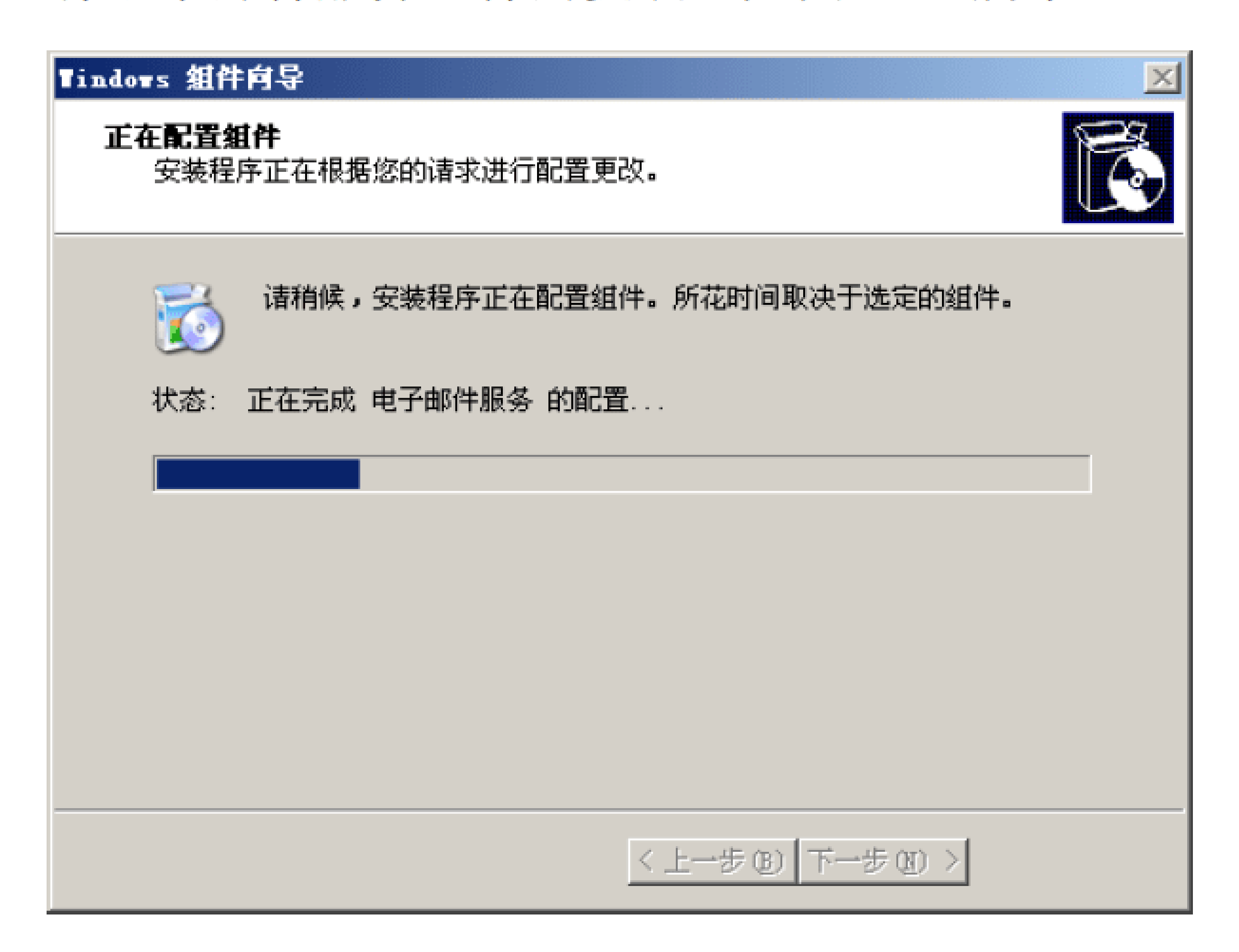


图 2-27 系统正在安装邮件服务器

(6) 安装完毕后，系统提示此服务器已经是邮件服务器了，如图 2-28 所示。单击【完成】按钮，邮件服务器就出现在【管理您的服务器】窗口中。



图 2-28 邮件服务器安装完成

2. 邮箱存储位置的设置

安装完成后，默认状态下系统将用户邮件存储在 C:\Inetpub\mailroot\Mailbox 文件夹中，通常需要将邮件的存储地址修改到一个空间比较大的存储位置，但要进行这样的修改需要有足够的权限，要由 Administrators 组中的成员来进行修改。设置邮件存储位置的操作如下。

(1) 在【管理您的服务器】窗口中单击【邮件服务器(POP3，SMTP)】中的【管理此邮件服务器】，系统显示【POP3 服务】控制台，如图 2-29 所示。

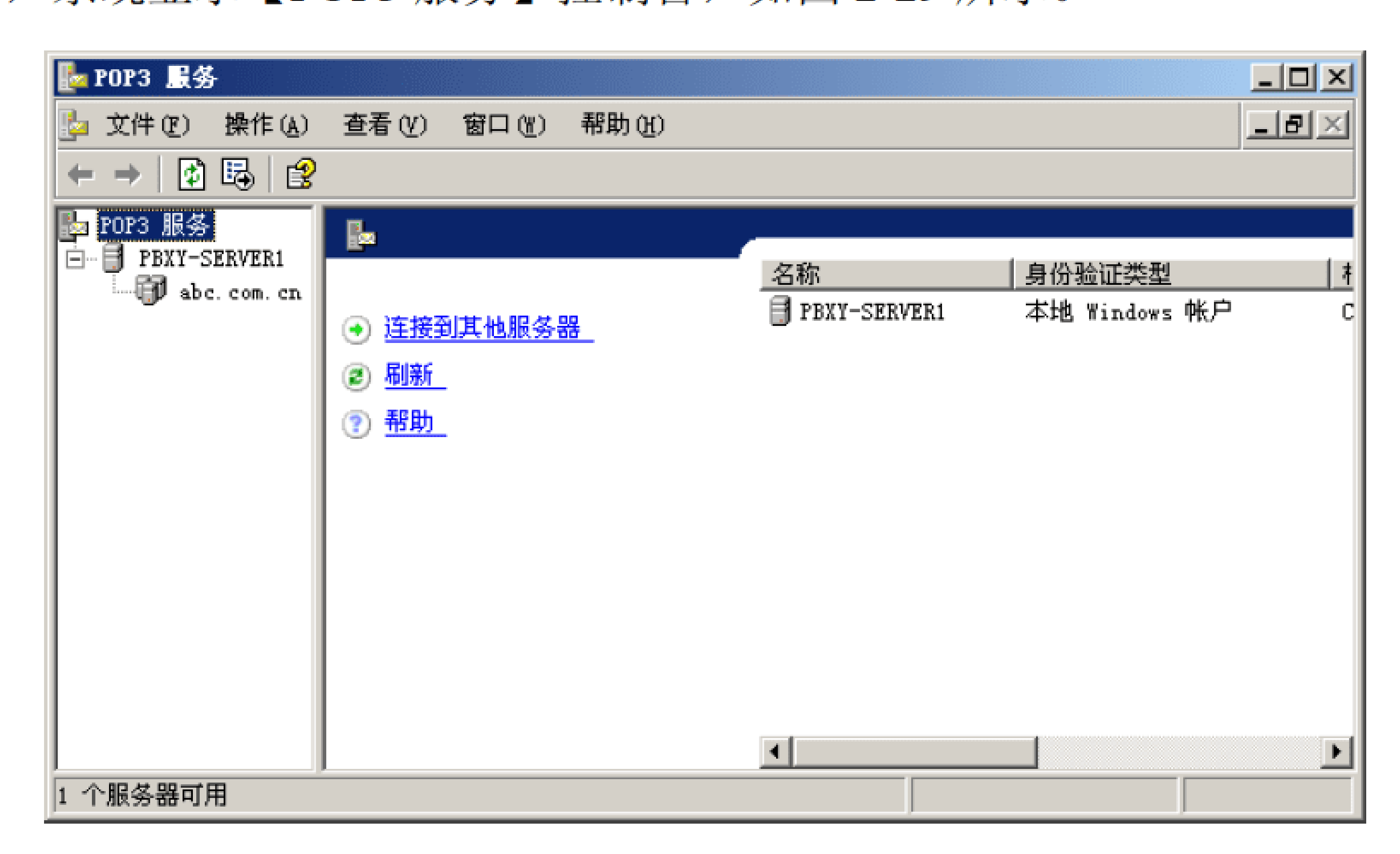


图 2-29　【POP3 服务】控制台

(2) 停止邮件服务器。右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【所有任务】|【停止】命令。

(3) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【属性】命令，系统显示邮件服务器的属性对话框。在【根邮件目录】文本框中输入邮件要存储的文件夹，或单击【浏览】按钮，选择邮件存储文件夹，如图 2-30 所示。

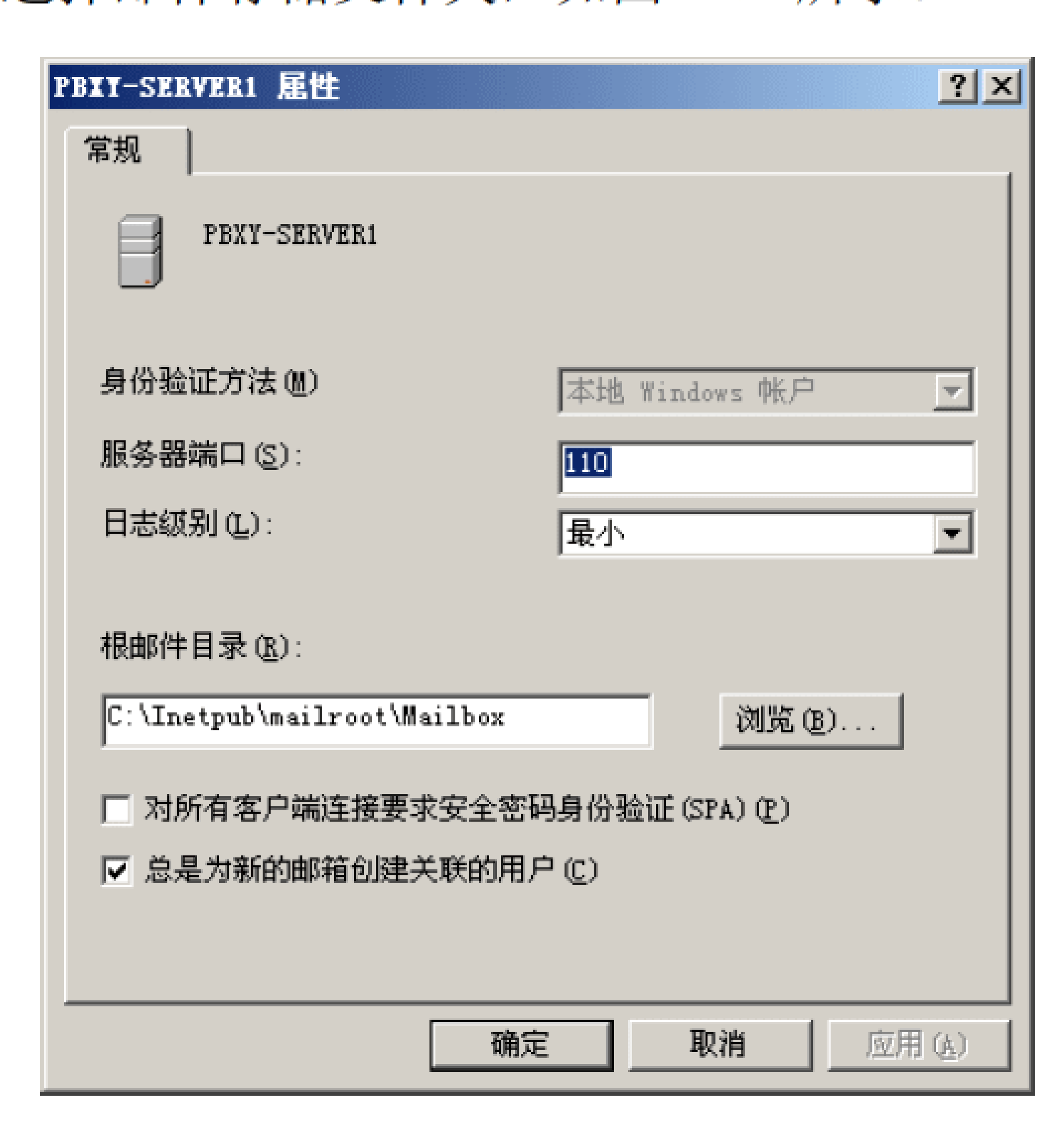


图 2-30　邮件服务器属性对话框

(4) 单击【确定】按钮，系统提示用户原有域无法存储邮件，需将域目录复制到新目录下，单击【确定】按钮，如图 2-31 所示。



图 2-31 配置邮件服务器提示(一)

(5) 系统提示重启邮件服务器，单击【是】按钮，如图 2-32 所示。



图 2-32 配置邮件服务器提示(二)

(6) 将系统默认状态下邮件存储文件夹如 C:\Inetpub\mailroot\Mailbox 中的域复制到新的邮件存储文件夹。

(7) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【所有任务】|【重启动】命令，启动邮件服务。

(8) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【刷新】命令，使新的域目录生效。

3. 域管理

邮件服务器中通过域来提供邮件服务。如果一个企业或单位需要多个域名，可以添加多个域名实现多邮件虚拟服务共享。

1) 创建域

(1) 打开【POP3 服务】控制台，右击计算机名称，在弹出的快捷菜单中选择【新建】|【域】命令，显示【添加域】对话框。

(2) 在【域名】文本框中输入新建域的名称，并确保该域名已在 DNS 服务器中设置好 MX 记录，如图 2-33 所示。

(3) 单击【确定】按钮，完成新域的添加。

2) 删除域

打开【POP3 服务】控制台，右击要删除的域，选择【删除】命令，然后单击【确定】按钮，即可删除该域。但是，若该域中有用户正连接到服务器，则不能删除该域。

3) 锁定/解除锁定域

通过锁定某个域，可阻止该域的其他成员检索自己的电子邮件。

打开【POP3 服务】控制台，右击要锁定的域，即可锁定该域；同样右击要解除锁定的域，即可解除该域锁定。

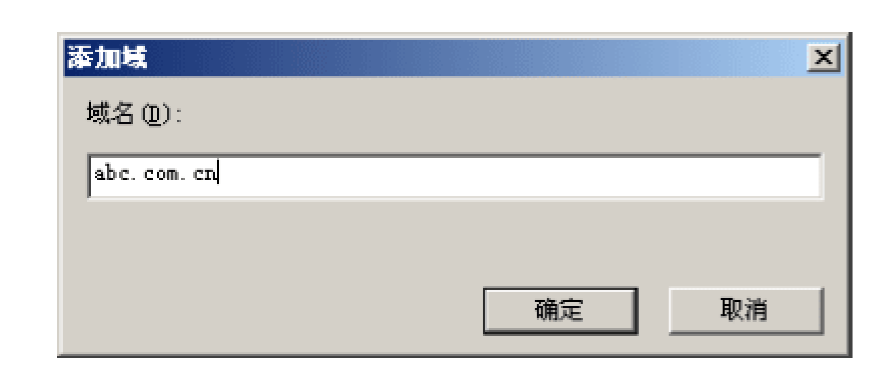


图 2-33　【添加域】对话框

4. 邮箱管理

1) 新建邮箱

在【POP3 服务】控制台中，右击要创建新邮箱的域，在弹出的快捷菜单中选择【新建】|【邮箱】命令，出现【添加邮箱】对话框。分别在【邮箱名】、【密码】、【确认密码】文本框中输入相应的内容，单击【确定】按钮，系统提示成功添加了一个名为 zhang 的邮箱，如图 2-34 所示。

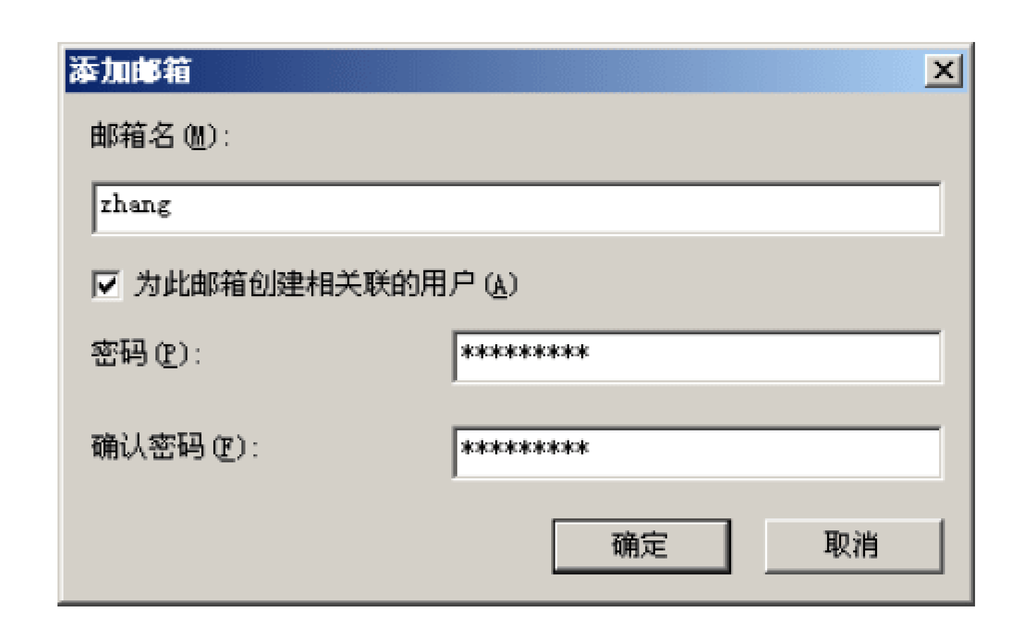


图 2-34　【添加邮箱】对话框

如图 2-35 所示，在名为 PBXY-SERVER1 的服务器上，创建了 abc.com.cn 域，在该域中创建了三个邮箱，分别是 zhang@abc.com.cn、taoan@abc.com.cn 和 liwenlong@abc.com.cn。

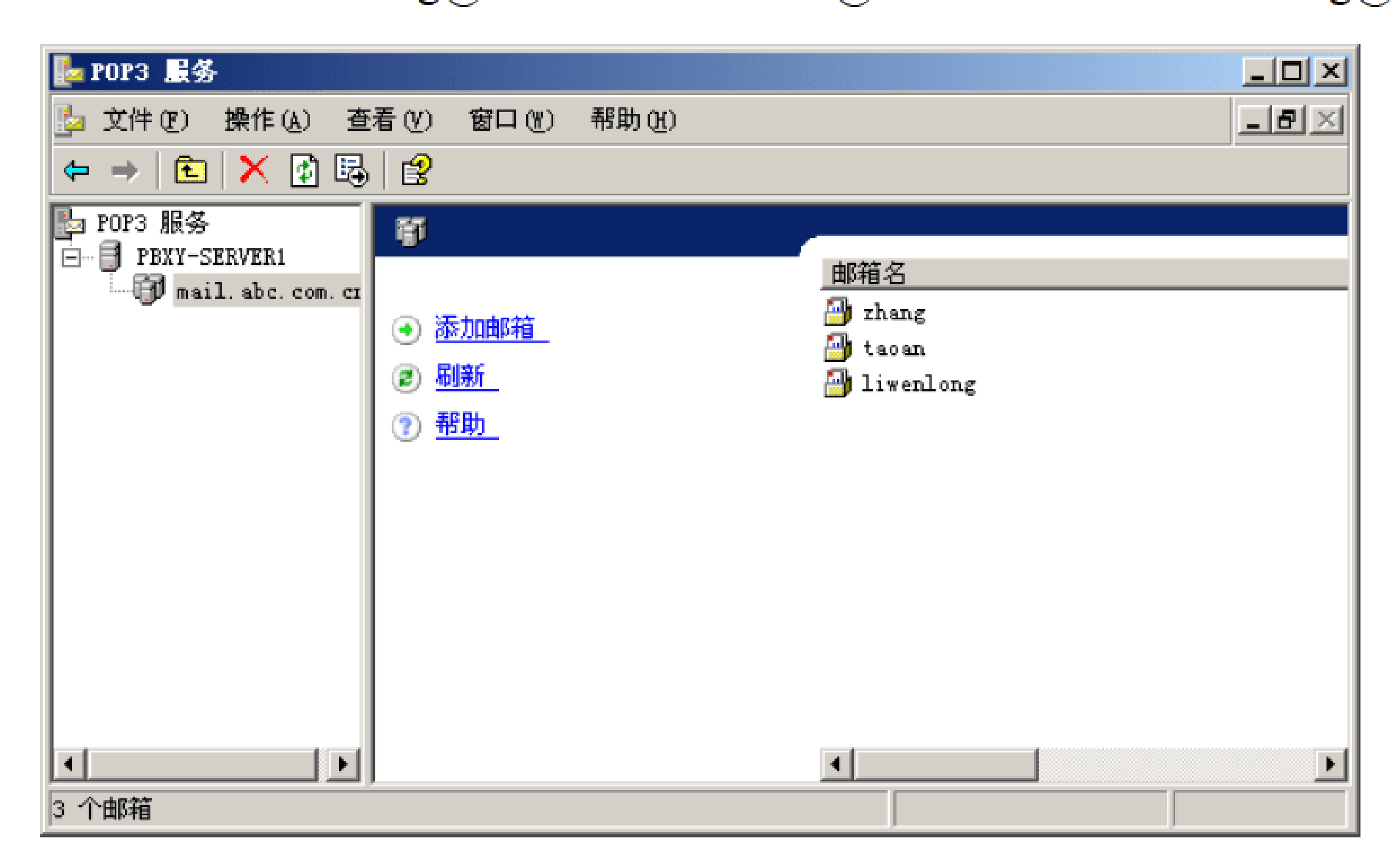


图 2-35　POP3 服务器配置结果

2) 删除邮箱

首先在域中右击欲删除的邮箱，然后在弹出的快捷菜单中选择【删除】命令，系统显

示【删除邮箱】对话框。若要同时删除与此邮箱相关联的用户帐户，则选中【删除】复选框。单击【确定】按钮，即可删除该邮箱。

此外，用户还可以根据需要进行邮箱的锁定、邮箱属性设置等邮箱的管理操作。

2.3.1.2 Linux 下电子邮件服务器的安装与配置

Linux 下电子邮件服务器的安装与配置主要包括两个服务器的安装与配置：一个是电子邮件传输服务器 Sendmail 的安装与配置；另一个是电子邮件阅读服务器 POP3 和 IMAP 的安装和配置。下面分别介绍这两个服务器的安装和配置过程。

1. 电子邮件传输服务器 Sendmail 的安装与配置

Sendmail 是一个使用最广泛的电子邮件传输服务器(MTA)。其历史可从 APARNET 时候开始。简单地说，Sendmail 的功能就是以 SMTP 传送邮件以及接收邮件。Sendmail 的程序非常复杂，设置复杂而功能强大，很多邮件服务器都使用 Sendmail。下面以 Red Hat Linux 7.0 为例介绍电子邮件传输服务器 Sendmail 的安装与配置。

1) Sendmail 的安装

由于 Red Hat Linux 7.0 已内置了 Sendmail，因此用户在安装 Linux 时，不需要另行安装。如果用户不能确定是否已经安装了 Sendmail，则可以执行以下命令检查：

```
#rpm -qa |grep sendmail
sendmail-8.11.6-3   //若出现此行，则表示已经安装了 Sendmail，"8.11.6-3"为版本号
```

如果用户发现系统未安装 Sendmail，则可以从网上下载 Sendmail 安装包，也可以在 Red Hat Linux 安装盘中找到 Sendmail 安装包。一般来说，需要安装以下 3 个安装包：主程序包、可供参考使用的配置文件、说明文档。安装命令如下：

```
#rpm -ivh sendmail-8.11.6-3.i386.rpm          //安装主程序包
#rpm -ivh sendmail-cf-8.11.6-3.i386.rpm       //安装可供参考使用的配置文件
#rpm -ivh sendmail-doc-8.11.6-3.i386.rpm      //安装说明文档
```

如果用户想从旧版本的 Sendmail 升级到新的版本，只需把执行参数“-i”改为“-U”即可。具体如下：

```
#rpm -Uvh sendmail-8.11.6-3.i386.rpm          //更新主程序包
```

2) Sendmail 的主要文件

以 Red Hat 7.0 为例，Sendmail RPM 包是 Sendmail 的 8.11.6-3 的版本。解包之后，主要的文件如表 2-2 所示。

表 2-2 Red Hat 7.0 中与 Sendmail 有关的文件(部分)

文 件	说 明
/etc/aliases /etc/aliases.db	别名文本(文件) 别名文件(数据库)
/usr/bin/newaliases	用于从/etc/aliases 生成/etc/aliases.db
/erc/mail/access /etc/mail/access.db	邮件传送的处理规则设置文件(文本) 邮件传送的处理规则设置文件(数据库)

续表

文　件	说　明
/etc/rc.d/init.d/sendmail /etc/sysconfig/sendmail	启动脚本
/usr/sbin/sendmail	Sendmail 程序
/usr/share/man/	手册目录
/etc/sendmail.cf	Sendmail 的配置文件
/var/log/statistics	日志文件
/var/spool/mqueue	邮件队列文件

3)　配置/etc/sendmail.cf 文件

Sendmail 的配置文件是 sendmail.cf，它包含了大部分的配置信息，控制着 Sendmail 的运行。sendmail.cf 也是一个文本文件，它主要有三个重要的功能。

- 定义 Sendmail 的环境。
- 按照接收邮件程序的语法重写地址。
- 从地址映射出传输邮件所必需的指令。

(1)　sendmail.cf 文件的结构

sendmail.cf 文件通常由一些节组成，常见的节如表 2-3 所示。

表 2-3　sendmail.cf 文件中常见的节

节　名	说　明	是否修改
本地信息(Local info)	定义单个主机的专用信息	是
通用宏(General macros)	定义有关本地网络的专用信息	是
类(Class)	定义用于特殊邮件传输程序的主机名群或域名群	否
版本号(Version Number)	标识 sendmail.cf 文件的版本号	是
专用宏(Special Macros)	定义由 Sendmail 所用的特殊的宏	否
选项(Options)	定义 Sendmail 的各个选项	否
报文优先值(Message Precedence)	定义 Sendmail 使用的各种报文的优先级值	否
可信任用户(Trusted Users)	定义在发送邮件时不检查发送者地址的用户	一般不
报头格式(Format of Header)	定义 Sendmail 插入邮件的报头格式	否
重写规则(Rewriting Rules)	定义重写邮件地址时使用的规则	一般不
邮件程序(Mailer)	定义 Sendmail 调用邮件传输程序时所使用的指令	否
置零规则(Ruleset Zero)	定义一组称为“置零规则”的特殊重写规则	一般不
置零规则中与其有关的部分(Machine-dependent Part of Rule- set Zero)	定义专用的置零规则部分，根据系统配置的邮件程序的不同而不同	一般不

(2)　Sendmail 的配置命令概述

sendmail.cf 文件的语法很难懂，因为其命令和变量都只有一个字符，且单个字符的命令

和一个字符的变量很容易造成混乱。

虽然这种语法非常难于理解，但是便于记忆，即每一行的第一个字符都是命令，根据这个字符就可以确定该命令是什么，从而也就可以确定它的结构。表 2-4 列出了 sendmail.cf 的语法和命令。

表 2-4　sendmail.cf 的配置命令

命　令	命令语法	命令含义
定义宏(D)	Dxvalue	设置宏变量 x 的值为 value(单值)
定义类(C)	Ccword1[word2],…	设置类变量 c 的值为 word1，word2，…
装载类(F)	Fcfile	从文件 file 中装入类(使用一个文件内容定义类变量)
设置选项(O)	Oovalue	设置选项 O 的值为 value
可信用户(T)	Tuser1[user2,…]	可信任用户是 user1，user2，…
设置优先级(P)	Pname=number	设置 name 的优先级为 number
定义邮件程序(M)	Mname，{field：value}	定义邮件程序 name
定义报头(H)	H[?mflag?]name：format	设置报头格式
设置规则集(S)	Sn	规则集 n 的开始
定义规则(R)	Rlhs rhs comment	将 lhs 格式改写为 rhs 格式

由于配置命令与它的变量或值之间没有空格，或用其他任何字符作间隔标志，因此使得这种“聚集在一起”的命令格式很难懂。例如：

```
DDxyz.com
```

这一行以字母 D 开始，也就是说这是一个宏定义命令。D 命令的变量应为宏的名字，由第二个字符指定，即定义了一个名为 D 的宏，宏 D 的值为 xyz.com。

(3)　sendmail.cf 文件的获得

由于 sendmail.cf 文件的配置极其复杂，所以没有人试图重新完整地编写一个 sendmail.cf 文件。在 Sendmail 的源代码分发中，为大多数的配置建立了模板文件。我们可以从模板文件中选择一个，再针对自己的需要作进一步修改。或者干脆用 Red Hat 7.0 中的 sendmail.cf 文件直接修改。

在提供的模板文件中，最常用的是 tcpproto.mc 文件，它直接用于与 TCP/IP 网络的连接。由于该模板文件是.mc 格式，所以需要下面的命令将其转换为.cf 格式：

```
#m4 tcpproto.mc >sendmail.cf
```

产生了 sendmail.cf 文件之后，用它覆盖/etc/目录下的 sendmail.cf 文件。

模板文件在结构上，一般遵从下列规则。

- 每台主机设置的“本地信息”通常位于文件的开头。
- 相同的命令通常集中在一起。
- 大部分文件都包含重写规则。
- 文件的最后可能包含着邮件程序的定义，并且掺杂着个别邮件程序的重写规则。

重要的是应该认识到，对于一个典型的系统，sendmail.cf 文件有多少需要修改之处。如

果选择了一个合适的样本文件，需要修改的内容则很少。从表 2-4 的第三列中的回答可以看到只需要修改和本地相关的一些信息。由此看来，Sendmail 的配置是一项很普通的任务。

在此不再罗列 Sendmail 的全部配置命令及其所有变量的意义，因为它实在是太多了，而且对于一个小型的局域网，只需按上面所说的，对模板文件稍加修改即可。

下面介绍一下经常需要修改的部分，在此以域名为 abc.com.cn，邮件服务器的主机名为 mail、邮件服务器 IP 地址以 210.45.12.30 为例。

① 修改主机名

将行：

```
Cwlocalhost
```

修改为：

```
Cwmail.abc.com.cn abc.com.cn
```

这里主要是定义邮件地址形式，说明本地既可接收地址为 XXX@mail.abc.com.cn，也可接收 XXX@abc.com.cn 的邮件。

这里说明一点，这一行不做修改也可以，因为在这行后面有一条：

```
Fw/etc/mail/local-host-names
```

它表明 w 类可从/etc/mail/local-host-names 文件中读取。/etc/mail/local-host-names 文件需要用户手工创建，并在该文件中定义本机的拥有的域名信息。其内容为

```
abc.com.cn
mail.abc.com.cn
```

② 定义域名

将行：

```
DM
```

修改为：

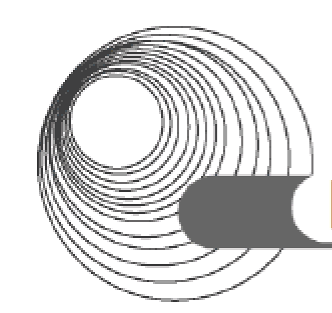
```
DMabc.com.cn
```

4) 配置/etc/mail/access 文件

/etc/mail/access 文件用于控制邮件传送的处理规则。下面是 Red Hat 7.0 中默认的/etc/mail/access 文件内容：

```
# Check the /usr/doc/sendmail-8.11.0/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/doc/sendmail-8.11.0/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain       RELAY
localhost                   RELAY
127.0.0.1                   RELAY
```

/etc/mail/access 文件的格式为




```
IpAddress|DomainName         RELAY|REJECT|OK|DISCARD
```

其中，RELAY 表示允许传送；REJECT 表示拒绝传送；OK 表示允许为拒绝域内的个别用户传送；DISCARD 表示丢弃。在这种情况下，邮件看上去是正常投递了，但是由于没有人接收，邮件会自动地“消失”在网络中。下面是一些例子：

```
202.99.11.120      RELAY          #允许为主机 202.99.11.120 传送
202.99.11          RELAY          #允许为网段 202.99.11 内的所有用户传送
abc.com.cn         RELAY          #允许为域 abc.com.cn 内的所有用户传送
xyz.com.cn         REJECT         #拒绝为域 xyz.com.cn 内的所有用户传送
abc.xyz.com.cn     OK             #允许为 abc.xyz.com.cn 传送
```

由于 Sendmail 并不直接读取/etc/access 文件，而是读取由该文件创建的数据库(.db)文件，因此在修改完该文件以后，应该使用下面的命令，使其生成相应的数据库文件：

```
#/usr/bin/makemap /etc/mail/access.db</etc/mail/access
```

在产生/etc/mail/access.db 文件后，用户不需要重新启动，所更改的设置值就会立即生效。此步骤也可以不做，但需要重新启动 Sendmail，因为 Sendmail 守护进程每次重新启动时都自动生成.db 文件。

5) 配置/etc/aliases 文件

别名是 Sendmail 最重要的功能之一，它的使用虽然简单，但却能发挥强大的功能。Sendmail 的别名被定义在 aliases 文件中，这个文件的位置是由 Sendmail 的配置文件 sendmail.cf 中的“O AliasFile=该文件的绝对路径”来指定的，一般名字是/etc/aliases。aliases 也是一个文本文件，其中的每一行的格式如下：

```
alias: recipient [, recipient]
```

其中，alias 为邮件地址中的用户名，而 recipient(收信人)是实际接收该邮件的用户。下面简单介绍定义别名的作用。

(1) 为单个用户指定别名

系统管理员可以为单个用户指定别名。指定别名的目的主要有两个：一是使用别名来保护合法用户的帐号不被泄漏。例如，用户王蕾的登录帐号设为 w457，而该用户对外的电子邮件帐号可以是 wanglei。由于两个帐号不同，则需要在别名文件中添加如下的行：

```
wanglei:           w457
```

二是使用别名来将约定俗成的邮件转给一个真实的用户。例如，在 Web 页中一般指定管理员电子邮件为 webmaster@abc.com.cn 或 administrator@abc.com.cn，但 webmaster 和 admininistrator 往往在系统中不是一个真实用户，邮件系统必须把它转给一个真正的系统管理员，如 Jim@abc.com.cn，则需要在别名文件中添加如下的两行：

```
webmaster:         jim
administrator:     jim
```

(2) 将发给特殊用户的邮件转发给实际用户。当系统守护进程(daemon)需要发信通知某个用户时，由于没有人能真正使用 daemon 的用户名登录，也就谈不上收信。因此，将邮件先发给假(pseudo)帐号，然后在转发给实际用户，如 root。例如：

```
bin:         root
daemon:      root
adm:         root
lp:          root
sync:        root
shutdown:    root
halt:        root
mail:        root
news:        root
uucp:        root
```

(3) 转发邮件

例如，主机 mail.abc.com.cn 上的用户 Kate 转到了另一家公司，其新帐号是 Kate@xyz.com.cn，那么，原公司的系统管理员可在别名文件中加入：

```
Kate:   Kate@xyz.com.cn
```

这样，发送到 Kate@abc.com.cn 的邮件会由主机 mail.abc.com.cn 自动转发到 Kate@xyz.com.cn。

(4) 实现邮件列表

别名最重要的功能就是实现邮件列表。有了邮件列表，在发送 E-mail 时，只要填写一个接收者地址就可以同时向多个人发信。例如，在别名文件中添加：

```
net_group:          Osmond, Tom, Stillman, Patrcko
owner-net_group:    Tom
```

那么，通过地址 net_group@abc.com.cn 就可以给网络组的全体成员 Osmond、Tom、Stillman 和 Patrcko 发信。第二行表示由 Tom 负责维护 net_group 这个邮件列表，若在传输信件给 net_group 时发生错误，就将有关的错误信息发送给 Tom。

由于 Sendmail 并不直接读取/etc/aliases 文件，而是读取由该文件创建的数据库(.dbm)文件，所以当修改完/etc/aliases 文件后，必须使用 newaliases 命令生成该数据库文件。

6) Sendmail 与域名系统的关系

电子邮件与域名系统的关系非常密切。在域名数据库中，有专门为电子邮件服务设置的 MX 记录。例如：

```
                IN     MX      10      mail
                IN     MX      20      mail1
mail            IN     A       202.99.11.120
mail1           IN     A       202.99.11.121
```

如果有一个 SMTP 客户要发送邮件给 XXX@abc.com.cn，它将查询 abc.com.cn 域中有关的 MX 记录。得到了上述信息后，它首先试图与具有较高邮件交换优先级(10)的主机 mail 发起 SMTP 连接。如果连接成功，就可以将信发送给 mail；如果连接失败，就试图与具有较低邮件交换优先级(20)的主机 mail1 发起 STMP 连接。如果连接成功，就可以将信发送给 mail1；而 mail1 接收到这封信后，就将其存放在邮件队列中，每隔一段时间就尝试将此信发送给 mail。在这个过程中，有关主机 mail 和 mail1 的 IP 地址将通过它们的 A 记录得到。必须注意，为了避免无限循环发送，MX 记录是非递归的。

7) 运行 Sendmail

Sendmail 在系统中是一个守护进程(daemon)，监听端口号为 25。通常在开机时就已经自动启动了。也可使用下面的命令启动或重新启动 Sendmail 守护进程。启动命令是：

```
#/etc/rc.d/init.d/sendmail start
```

若对配置文件修改后，使其生效，可以重新启动 Sendmail 守护进程，命令是：

```
#/etc/rc.d/init.d/sendmail restart
```

如果设定 Sendmail 服务在计算机启动时自动启动或不启动，可以使用 ntsysv 命令将它加到引导程序中，也可以通过 chkconfig 命令来设定，该命令格式是：

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如，我们希望计算机启动运行级别 3、5 时启动 Sendmail 服务，则命令为

```
#chkconfig --level 35 sendmail on
```

再如，我们希望计算机启动运行级别 4 时不启动 Sendmail 服务，则命令为

```
#chkconfig --level 4 sendmail off
```

如果希望在任务运行级别下都启动或不启动 Sendmail 服务，只需不设定“[--level <运行级>]”就可以了，即

```
#chkconfig sendmail on
#chkconfig sendmail off
```

8) 测试 Sendmail 服务

启动 Sendmail 之后，接下来需要测试 Sendmail 是否能正常工作。由于 Sendmail 默认的通信端口为 25，所以可以利用 telnet 命令登录到第 25 号端口，测试 Sendmail 是否已经启动。其命令为

```
#telnet localhost 25
```

如果用户可以看到登录信息，则表示 Sendmail 已经启动了。

2. 电子邮件阅读服务器 POP3 和 IMAP 的安装和配置

如果已经正确地安装了 Sendmail 服务器，用户就可以登录到邮件主机进行读或写邮件了。但现在 Windows 用户都习惯于使用如 Outlook Express 这样的电子邮件客户端软件来接收和发送邮件，这就需要在邮件主机中增加电子邮件阅读服务器。电子邮件阅读服务器主要有两种：一种是 POP3(Post Office Protocol，即邮局协议，3 表示第 3 版)服务器，另一种是 IMAP(Internet Message Access Protocol，因特网报文存取协议)服务器。

1) 安装 POP3 和 IMAP 服务器

如果用户在安装 Linux 时已经安装了 POP3 和 IMAP 服务器程序 ipop3d 和 imapd，就不需要另行安装。但如果不确定已经安装了 ipop3d 和 imapd，则可执行以下命令确认：

```
#rpm -qa |grep imap
imap-2000c-15   //若出现此行，则表示已经安装了 POP3 和 IMAP 服务器
```

如果用户发现系统未安装 POP3 或 IMAP 服务器软件，则可以从网上下载相应的安装包，也可以在 Red Hat Linux 安装盘中找到这两种服务器的安装包。然后执行以下命令：

```
#rpm -ivh imap-2000c-15.i386.rpm   //安装 imap 软件包
```

如果从旧版本升级至新版本，则只需要把执行参数“-i”改为“-U”即可：

```
#rpm -ivh imap-2000c-15.i386.rpm   //安装 imap 软件包
```

这里需要说明一点，由于 Red Hat Linux 将 POP3 和 IMAP 程序编成了一个 imap 组件，因此只需安装这个组件即可。安装完成之后，在/usr/sbin/目录中就可以找到 imapd、ipop2d 和 ipop3d 这 3 个文件，每个文件的文件名都以“d”结尾表示 daemon(守护程序)。

2)　设置和启动 POP3 和 IMAP 服务器

安装好 POP3 和 IMAP 服务器之后，需要修改配置文件。

(1)　修改/etc/services

需要确定/etc/services 文件有以下几行内容，同时这些内容未被加上注释符“#”：

```
pop2            109/tcp     pop-2       postoffice
pop2            109/udp     pop-2
pop3            110/tcp     pop-3
pop3            110/udp     pop-3
imap            143/tcp     imap2
imap            143/udp     imap2
```

(2)　修改/etc/xinetd.d/ipop3 和/etc/xinetd.d/imap 文件

如果要启动 pop3 服务，则需要修改/etc/xinetd.d/ipop3，把 disable 的值 yes 改成 no。这个文件内容大致如下：

```
service pop3
{
        disable = no                         //将 yes 改为 no，表示启动该服务
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/ipop3d
        log_on_success    += HOST DURATION
        log_on_failure    += HOST
}
```

以同样的方法修改/etc/xinetd.d/imap 文件，启动 imap 服务。

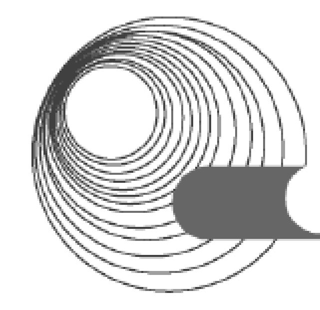
(3)　重新启动 xinetd

要想修改内容立即生效，可以重新启动 xinetd 程序。命令是：

```
#/etc/rc.d/init.d/xinetd restart
```

3)　测试 POP3 和 IMAP 服务器

与测试 Sendmail 服务器一样，可以通过 telnet 命令分别登录到 110 端口来测试 POP3 服务器，登录到 143 端口来测试 IMAP 服务器。其命令分别是：




```
#telnet localhost 110            //测试 POP3 服务器
#telnet localhost 143            //测试 IMAP 服务器
```

如果登录成功，则表明该服务器已成功安装并启动。

2.3.2 典型例题分析

阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 5 月下午试题二)

【说明】

在 Windows Server 2003 系统中，经常采用系统自带组件进行邮件服务器的配置。某邮件服务器部分信息如表 2-5 所示。

表 2-5 某邮件服务器部分信息

存放位置	D:\mailbox
IP 地址	210.120.112.38
用户 Alice 的邮箱	Alice@software.com

要求采用域用户来代替独立的用户，通过组策略赋予或限制一定的用户使用某应用系统或数据资源的权限。图 2-36 为邮件服务器配置中 POP3 服务身份认证和邮件域名配置窗口；图 2-37 为 POP3 服务常规属性窗口。

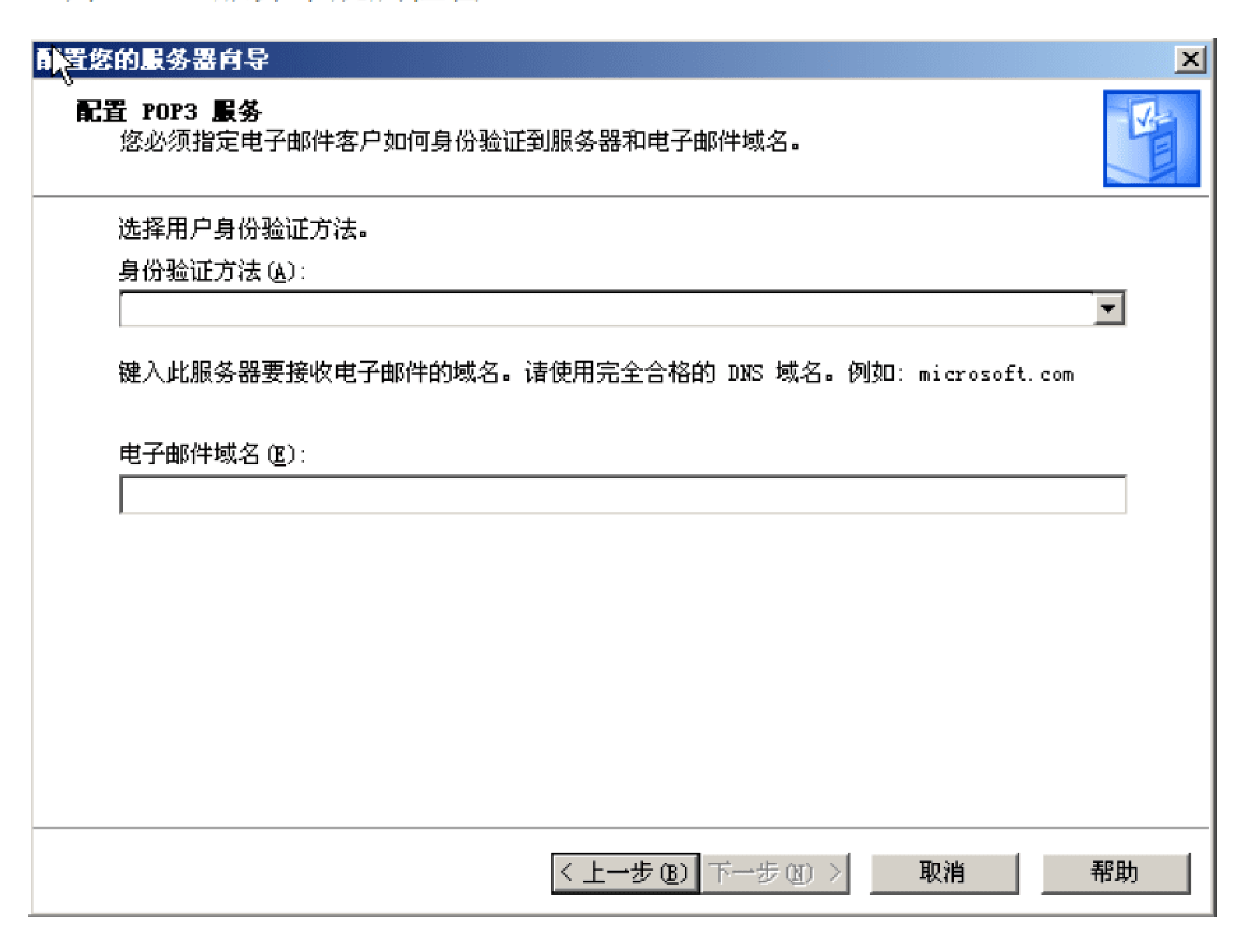


图 2-36 【配置 POP3 服务】界面

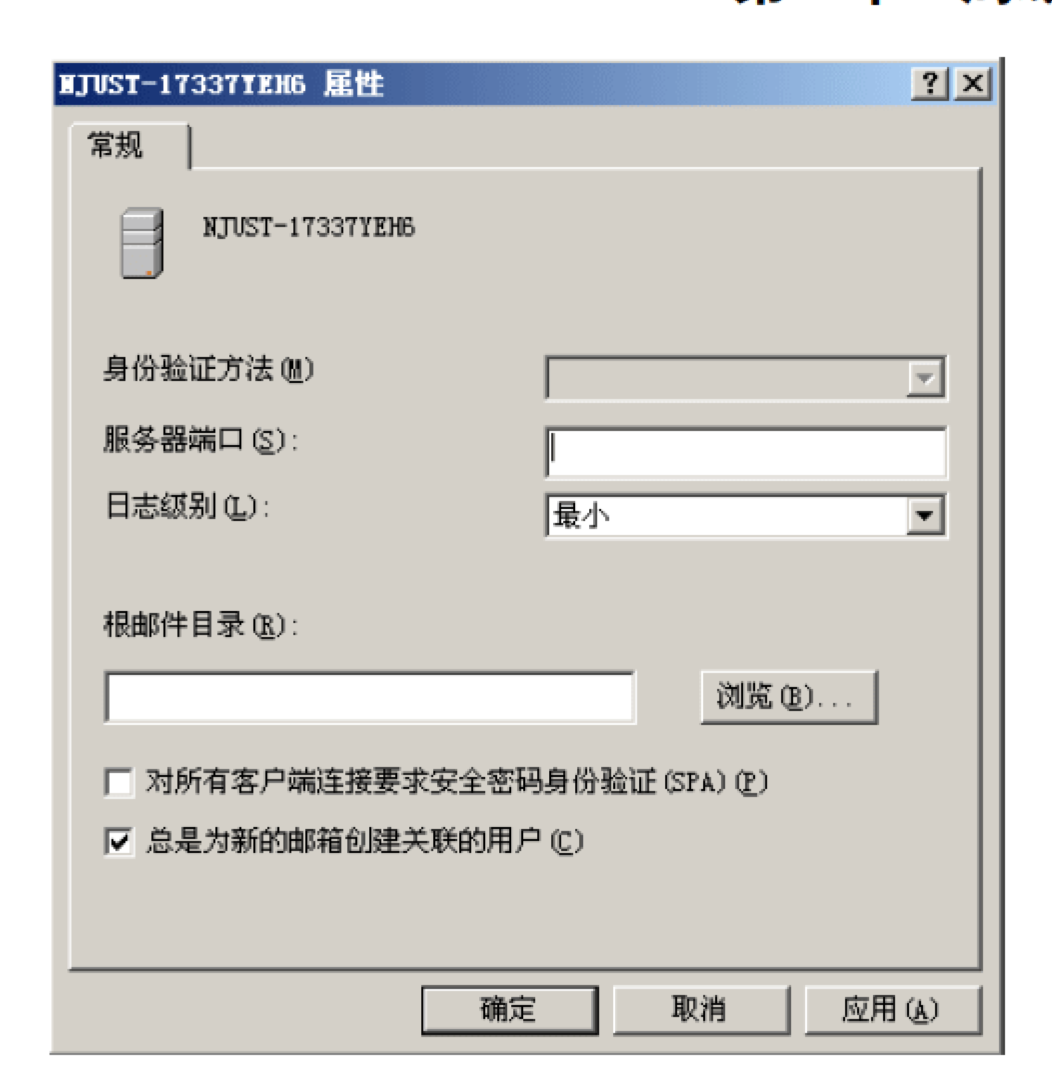


图 2-37　【常规】选项卡

客户端电子邮件服务器配置窗口如图 2-38 所示。

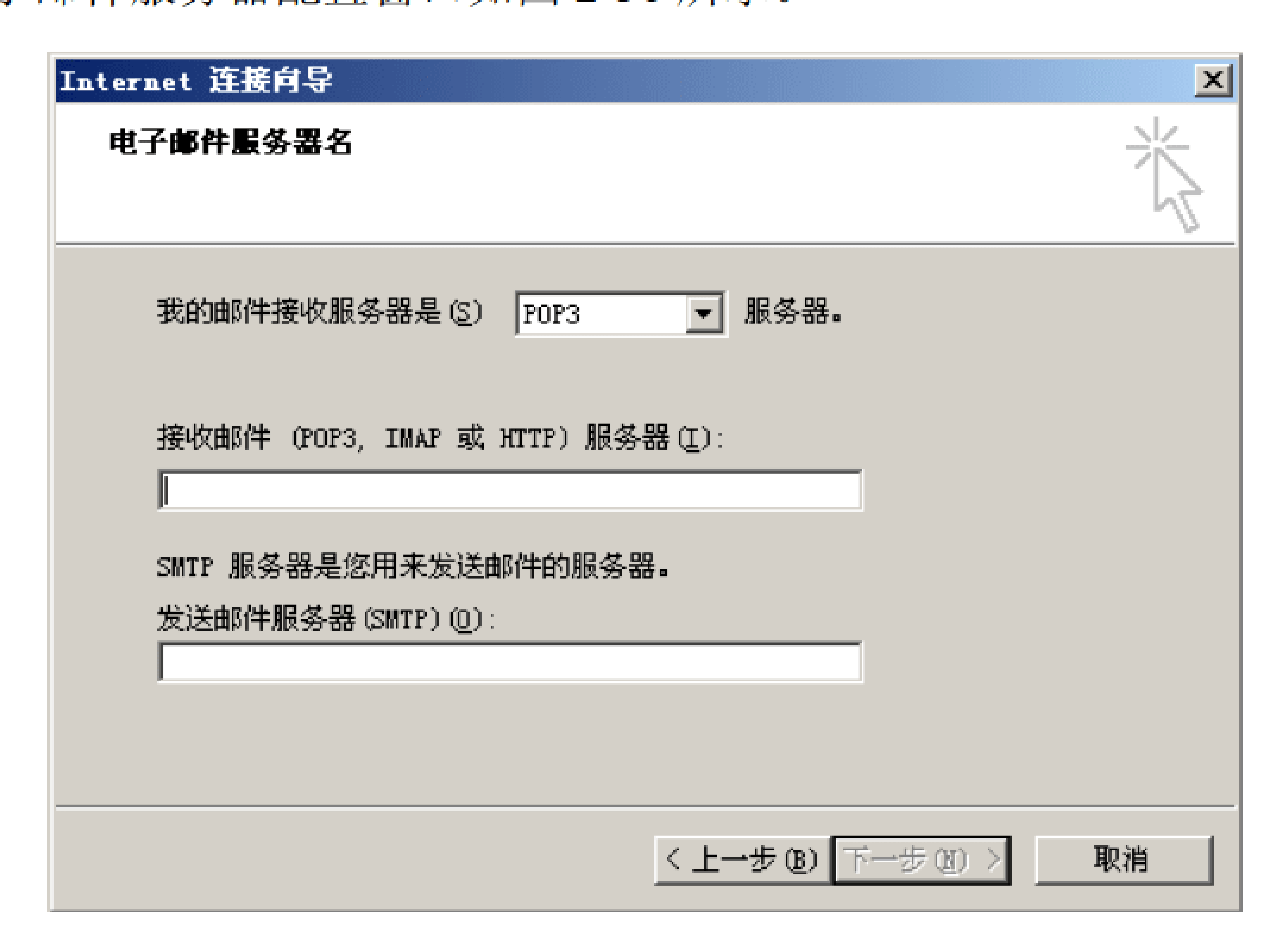


图 2-38　【电子邮件服务器名】界面

【问题 1】(3 分)

邮件服务器的配置有以下几个步骤，正确的安装顺序为：__(1)__。

A. 设置邮件服务器端口、邮箱根目录、认证方式

B. 在邮件服务器中添加域、用户

C. 在邮件客户端软件中配置用户邮件

D. 利用【配置您的服务器向导】安装相关组件

【问题 2】(4 分)

图 2-36 中【身份验证方法】下拉列表框中应选择__(2)__。

A. Active Directory 集成的　　B. Windows 集成的

C. 加密的密码文件　　D. 用户名及密码

【电子邮件域名】文本框中应填入__(3)__。

【问题3】(4分)

图2-37中默认情况下，【服务器端口】文本框中应填入__(4)__，【根邮件目录】文本框中应填入__(5)__。

【问题4】(4分)

图2-38中【接收邮件服务器】文本框中应填入__(6)__，【发送邮件服务器】文本框中应填入__(7)__。

分析：

【问题1】安装邮件服务器的操作步骤如下。

① 利用【配置您的服务器向导】安装邮件服务器。依次选择【开始】|【管理工具】|【管理您的服务器】命令，在弹出的窗口中单击【添加或删除角色】链接，单击【下一步】按钮。打开【服务器角色】对话框，选中【邮件服务器】选项，单击【下一步】按钮。系统弹出【配置POP3服务】界面，选择身份验证方法，填写电子邮件域名，单击【下一步】按钮。弹出【选择总结】界面，单击【下一步】按钮。按系统提示插入光盘，系统自动进行电子邮件服务的安装。

② 设置邮件服务器端口、邮箱根目录、认证方式。在【管理您的服务器】窗口中单击【邮件服务器(POP3，SMTP)】中的【管理此邮件服务器】，系统打开【POP3服务】控制台。右击【POP3服务】下的计算机名称，选择【所有任务】|【停止】命令。然后右击【POP3服务】下的计算机名称，选择【属性】命令，打开属性对话框，可以设置服务器端口、邮箱根目录等。

③ 在邮件服务器中添加域、用户。打开【POP3服务】控制台。右击【POP3服务】下的计算机名称，选择【新建】|【域】命令，打开【新建域】对话框。输入域名，单击【确定】按钮，完成域的添加。然后在【POP3服务】控制台中右击要创建新邮箱的域，选择【新建】|【邮箱】命令，弹出【添加邮箱】对话框。输入【邮箱名】、【密码】、【确认密码】，单击【确定】按钮，即可添加邮箱。

④ 在邮件客户端软件中配置用户邮件。如在Outlook中创建帐户，进行邮件的收发。

【问题2】Windows Server 2003 家族产品支持下表所列的身份验证方法：本地Windows帐户、Active Directory 集成的、加密的密码文件。

如果局域网中已经事先设立了一个域，并且有大量的用户帐户，建议选择“Active Directory 集成的”，这样用户就可以使用原有的登录帐号和密码来处理电子邮件了；如果邮件服务器不是活动目录域的成员，并且希望在安装了邮件服务的本地计算机上存储用户帐户，那么可以使用“本地Windows帐户”身份验证方法来进行邮件服务的用户身份验证。本地Windows帐户身份验证将邮件服务集成到本地计算机的安全帐户管理器(SAM)中。通过使用安全帐户管理器，在本地计算机上拥有用户帐户的用户就可使用与由POP3服务提供的或本地计算机进行身份验证的相同的用户名和密码。“加密的密码文件”身份验证对于还没有安装活动目录，并且又不想在本地计算机上创建用户的大规模部署来说十分理想，同时从一台本地计算机上就可以很轻松地管理可能存在的大量帐户。

【问题3】POP3默认的TCP端口为110，所以默认情况下【服务器端口】文本框中的内容是110。由题目知，邮箱存放的位置是D:\mailbox，也就是说【根邮件目录】是

D:\mailbox。

【问题 4】客户端软件使用 POP3 协议访问并读取邮件服务器上的信息，使用 IMAP 协议将邮件发送到发方的邮件服务器。因此【接收邮件服务器】文本框中应填入 pop3@software.com，【发送邮件服务器】文本框中应填入 imap@ software.com。

答案：

【问题 1】(1) D→A→B→C

【问题 2】(2) A　　(3) software.com

【问题 3】(4) 110　　(5) D:\mailbox

【问题 4】(6) pop3@software.com　　(7) imap@ software.com

2.3.3　同步练习

阅读以下说明，回答问题 1～问题 5，将答案填入对应的答案栏内。

【说明】

在 Linux 下安装与配置 Sendmail 服务，Sendmail 服务程序需要读取一些配置文件，以下列出了 Sendmail 的 3 个配置文件的主要内容。

- /etc/mail/local-host-names 文件内容：

```
xyz.com.cn
mail.xyz.com.cn
```

- /etc/mail/access 文件内容：

```
localhost.localdomain       RELAY
localhost                   RELAY
127.0.0.1                   RELAY
210.45.12                   RELAY
xyz.com.cn                  RELAY
210.45.13                   REJECT
abc.com.cn                  REJECT
```

- /etc/aliases 文件内容：

```
bin:            root
daemon:         root
adm:            root
lp:             root
sync:           root
shutdown:       root
halt:           root
mail:           root
news:           root
uucp:           root
webmaster:      tom
jack:           jack@sohu.com.cn
net_group:      Osmond, Tom, Stillman, Patrcko
```

```
owner-net_group: Tom
```

【问题 1】该电子邮件服务器将接收电子邮件地址格式是什么样的电子邮件？用户名使用 XXXX 代替，写出完整格式(假设 DNS 已作解析)。

【问题 2】该电子邮件服务器将允许传送哪个网络和哪个域的电子邮件？该电子邮件服务器将拒绝传送哪个网络和哪个域的电子邮件？

【问题 3】该电子邮件服务器收到一封寄给 webmaster@xyz.com.cn 的邮件时，作何处理？该电子邮件服务器收到一封寄给 net_group@xyz.com.cn 的邮件时，又作何处理？

【问题 4】命令#/usr/bin/makemap /etc/mail/access.db</etc/mail/access 的作用是什么？

【问题 5】当对 Sendmail 的配置文件作修改后，怎样使配置文件立即生效(不重新启动计算机)？

2.3.4 同步练习参考答案

【问题 1】XXXX@ xyz.com.cn、XXXX@mail.xyz.com.cn。

【问题 2】允许网络 210.45.12.0/24 和域 xyz.com.cn 内所有用户的电子邮件的传送，拒绝网络 210.45.13.0/24 和域 abc.com.cn 内所有用户的电子邮件的传送。

【问题 3】该电子邮件服务器收到一封寄给 webmaster@xyz.com.cn 的邮件时，将邮件传输给用户名为 Tom 的用户；当电子邮件服务器收到一封寄给 net_group @xyz.com.cn 的邮件时，将邮件传输给用户名为 Osmond、Tom、Stillman、Patrcko 的用户各一份。

【问题 4】创建传送控制配置文件 access 相应的数据库文件。

【问题 5】#/etc/rc.d/init.d/sendmail restart。

2.4 FTP 服务器

2.4.1 考点辅导

2.4.1.1 Windows Server 2003 的 IIS 下 FTP 服务器的安装与配置

1. FTP 服务器的安装

Windows Server 2003 中 IIS 里内置了 FTP 服务模块，安装比较简单。由于 FTP 不是默认的安装组件，系统不会自动安装，因此必须采用 Windows 组件方式来安装 FTP 服务。具体操作步骤如下。

(1) 选择【开始】|【设置】|【控制面板】命令，打开控制面板窗口，双击【添加/删除程序】图标，选择【添加/删除 Windows 组件】选项。

(2) 在【Windows 组件向导】对话框的列表框中选中【应用程序服务器】复选框，如图 2-39 所示。

(3) 单击【详细信息】按钮，弹出【应用程序服务器】对话框，选中【Internet 信息服务(IIS)】复选框，如图 2-40 所示。



图 2-39 【Windows 组件向导】对话框

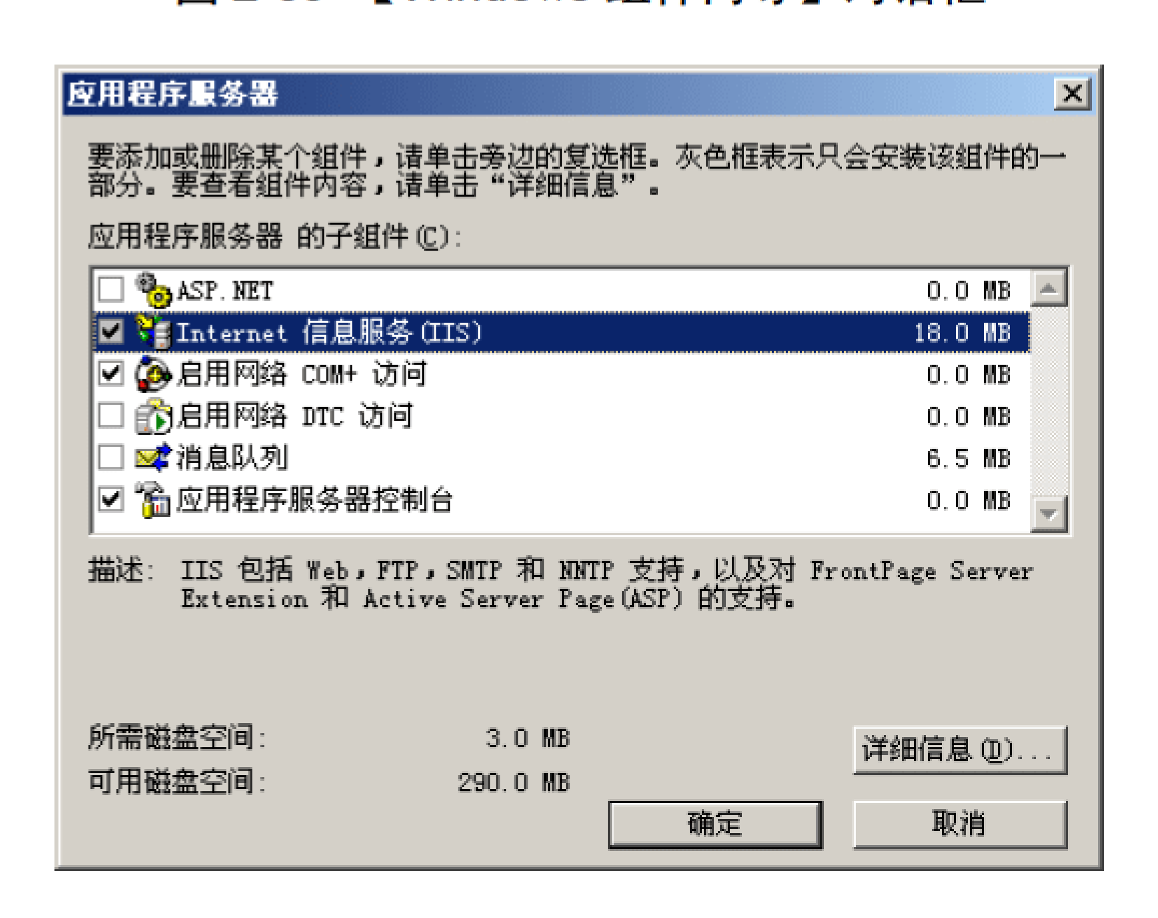


图 2-40　【应用程序服务器】对话框

(4) 在【应用程序服务器】对话框中单击【详细信息】按钮，显示【Internet 信息服务(IIS)】对话框，选中【文件传输协议(FTP)服务】复选框，单击【确定】按钮，按提示信息插入光盘，系统自动完成 FTP 服务的安装，如图 2-41 所示。

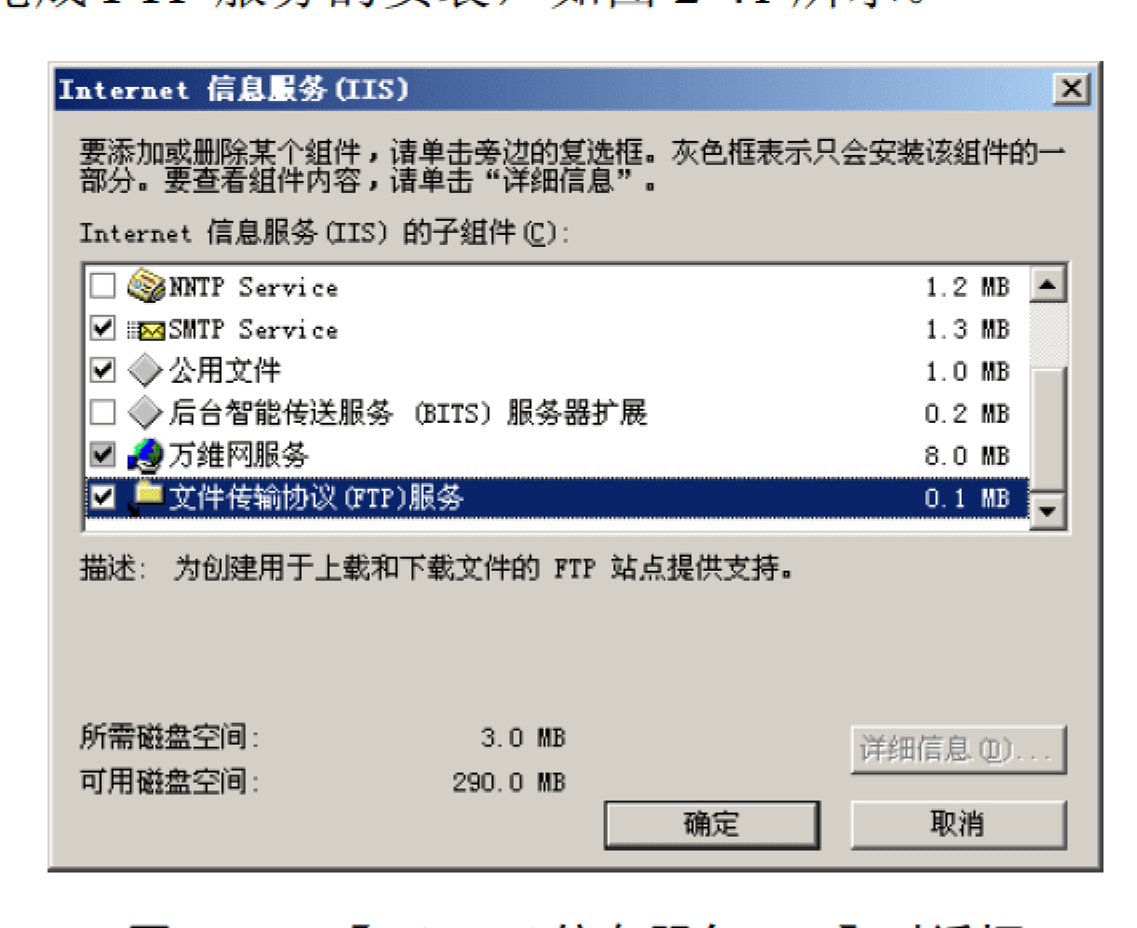


图 2-41　【Internet 信息服务(IIS)】对话框

2. FTP 服务器的配置

FTP 服务器的“默认 FTP 站点”所在主目录为 C:\Inetpub\ftproot(若系统安装在 D 盘，则为 D:\Inetpub\ftproot)，IP 地址为“全部未分配”，允许来自任何 IP 地址的用户以匿名方式访问。只需要将共享文件复制到 C:\Inetpub\ftproot 目录下，FTP 客户端用户就可以匿名登录进行文件下载，但由于默认情况下主目录为只读方式，所以客户端只能下载而不能上传。为了更好地管理 FTP 服务器，需要对它进行适当的配置，方式如下。

1) 修改 IP 地址和端口

(1) 依次选择【开始】|【管理工具】|【Internet 信息服务(IIS)管理器】命令，打开 IIS 控制台，显示 IIS 信息，包括 FTP 站点、应用程序池、网站以及 Web 服务扩展等，如图 2-42 所示。

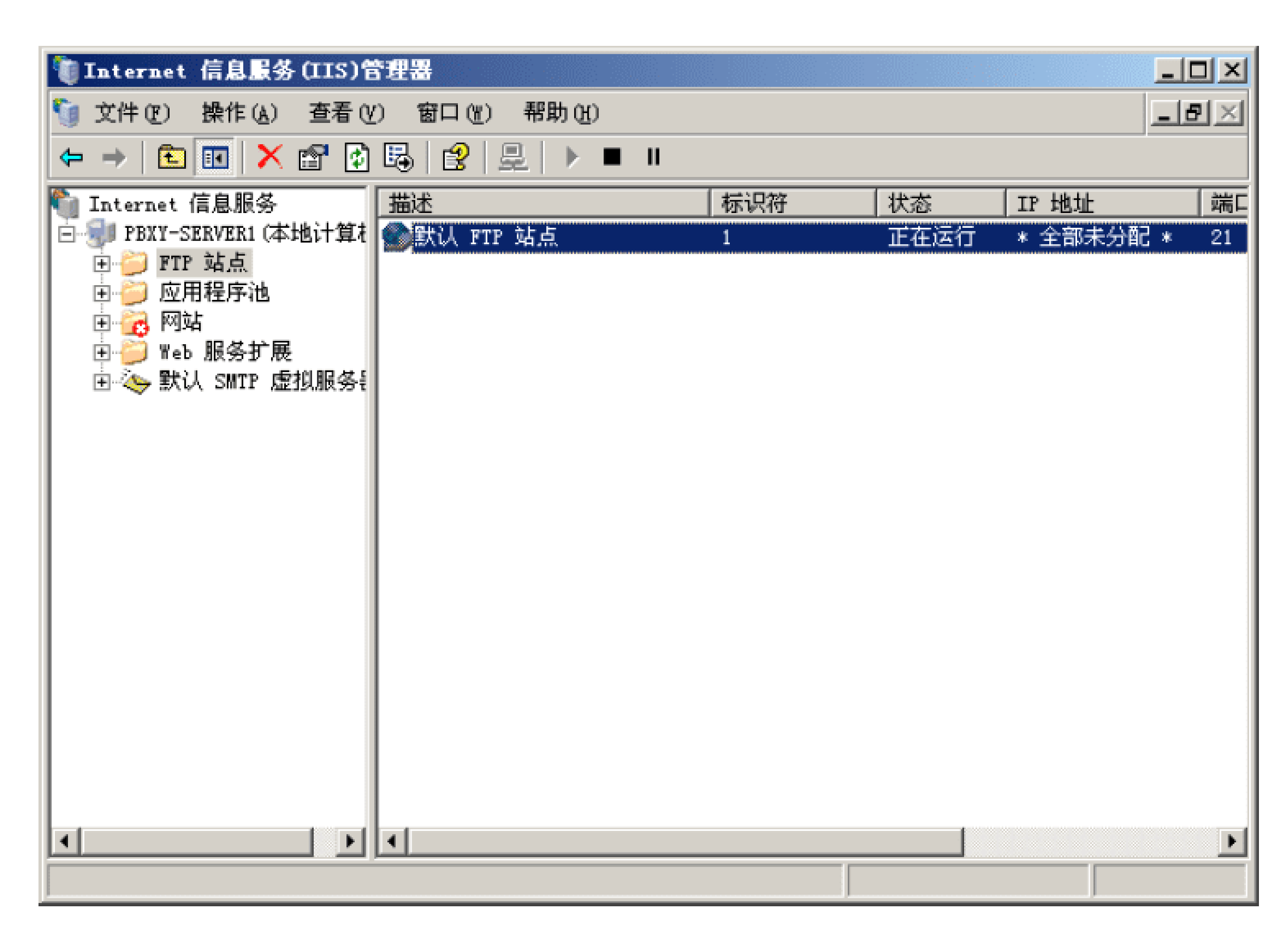


图 2-42 IIS 控制台

(2) 展开窗口左边的【FTP 站点】控制树，选中【默认 FTP 站点】选项，单击工具条上的相应按钮可以实现对 FTP 站点的启动、暂停、停止等操作。

(3) 右击相应站点，在弹出的快捷菜单中选择【属性】命令，系统将显示 FTP 站点属性信息，如图 2-43 所示。其中【FTP 站点】选项卡包括 FTP 站点标识，FTP 站点连接和日志记录等信息。其中 IP 地址和端口号在 FTP 站点标识中设置。

【描述】作为 FTP 服务器的名称显示在“Internet 信息服务”窗口的目录中。如果在一台计算机中安装了多个 FTP 服务器，管理员可根据“标识”对各台 FTP 服务器加以区分。

【IP 地址】下拉列表框用于设置该 FTP 站点的 IP 地址。Windows Server 2003 操作系统中允许安装多块网卡，而且每块网卡也可以绑定多个 IP 地址。通过设置【IP 地址】文本框中的信息，FTP 客户端利用设置的这个 IP 地址来访问该 FTP 服务器。通过该下拉列表框从一个或多个地址中选择一个作为“IP 地址”。

【TCP 端口】是指用户与 FTP 服务器进行连接并访问的端口号，默认的端口号为 21。服务器也可设置一个任意的 TCP 端口号，若更改了 TCP 端口号，客户端在访问时需要在 URL 之后加上这个端口号，因此必须让客户端事先知道，否则就无法进行 TCP 连接。

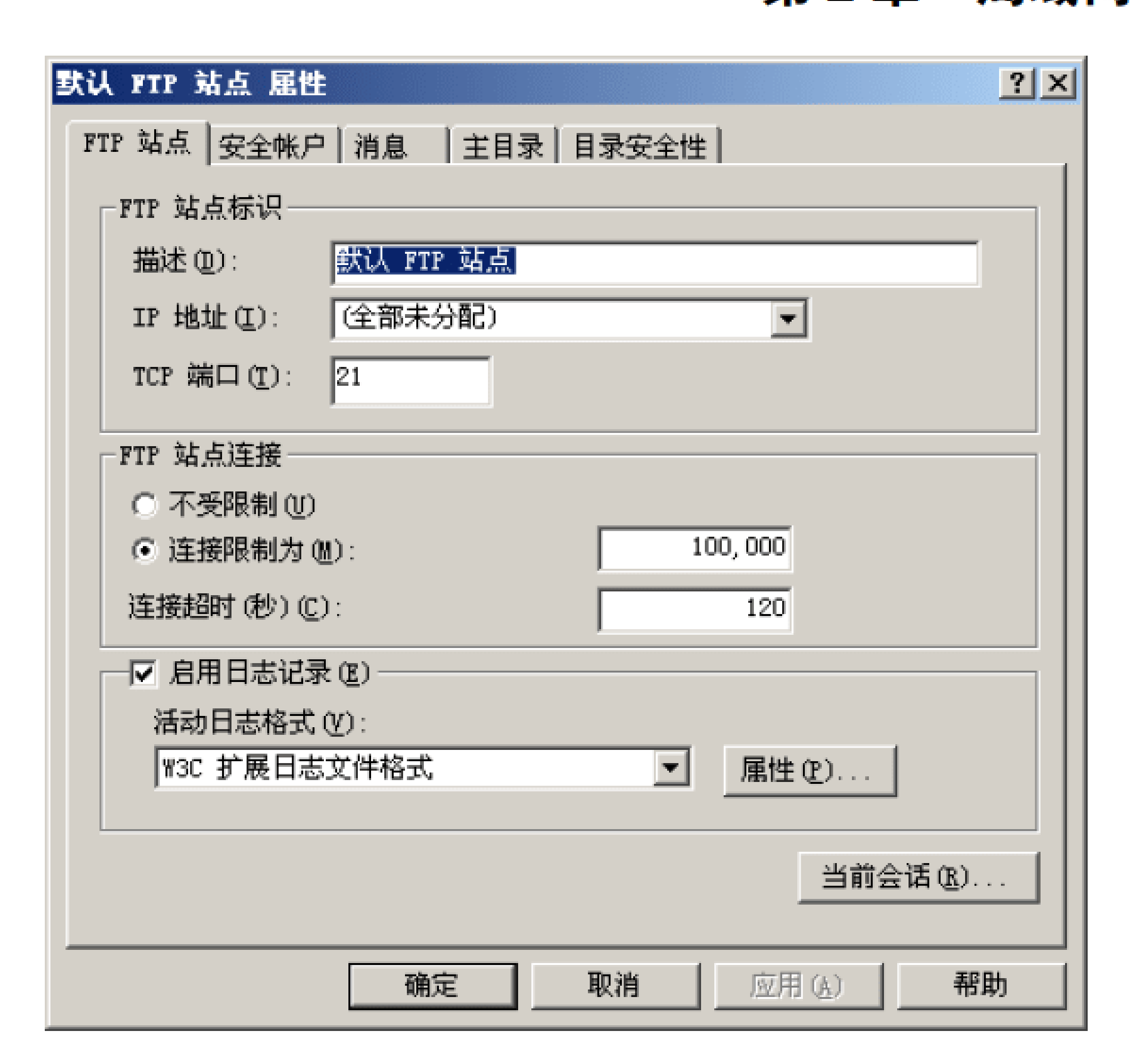


图 2-43 FTP 站点属性设置

比如，可以设置标识为 MP3，IP 地址为 192.168.0.61，端口号为 21，如图 2-44 所示。

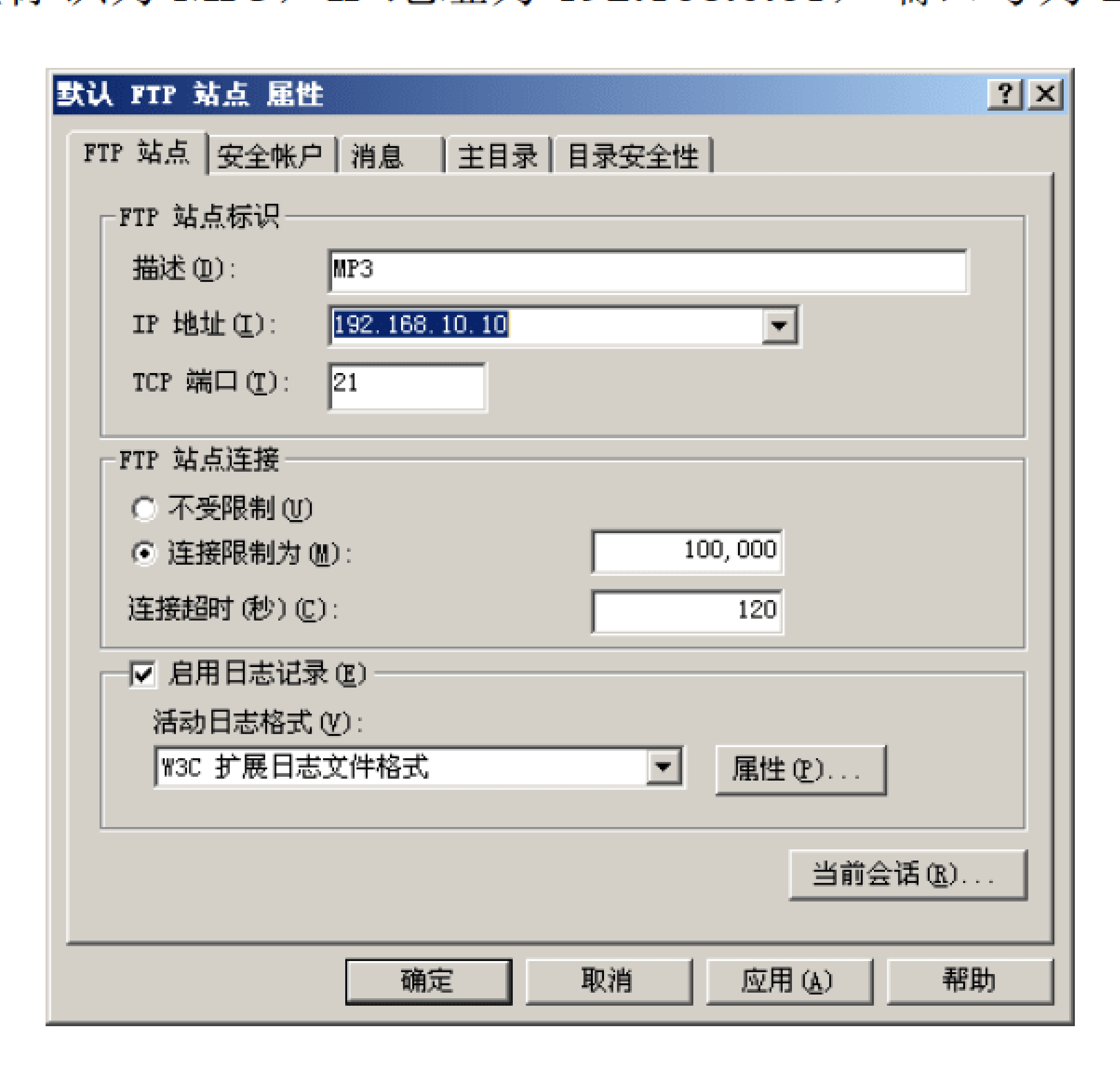


图 2-44 配置后的 FTP 站点属性

2) 限制连接数量

在【FTP 站点】选项卡的【FTP 站点连接】中有以下 3 个选项。

(1) 【不受限制】：该选项允许同时发生的连接数将不受任何限制。

(2) 【连接限制为】：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。

(3) 【连接超时】：当连接超时达到某一时间，服务器就自动断开该连接。

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。同时，为了确保 FTP 协议在连接失败时关闭连接，因此需要设置连接超时。

3) 设置主目录

主目录信息在属性信息的【主目录】选项卡中设置。所谓主目录是指映射为 FTP 根目录的文件夹，FTP 站点中的所有文件将保存在该目录中。系统默认的 FTP 主目录为 C:\Inetpub\ftproot (其中，C 为操作系统安装的逻辑盘符，若系统安装在 D 盘，则为 D)，可以根据用户的需要更改主目录和其属性。

可以把主目录修改为计算机中的其他文件夹，甚至可以是另一台计算机上的共享文件夹。同时，管理者可以修改用户对站点的访问权限，以及目录的列表风格，如图 2-45 所示。

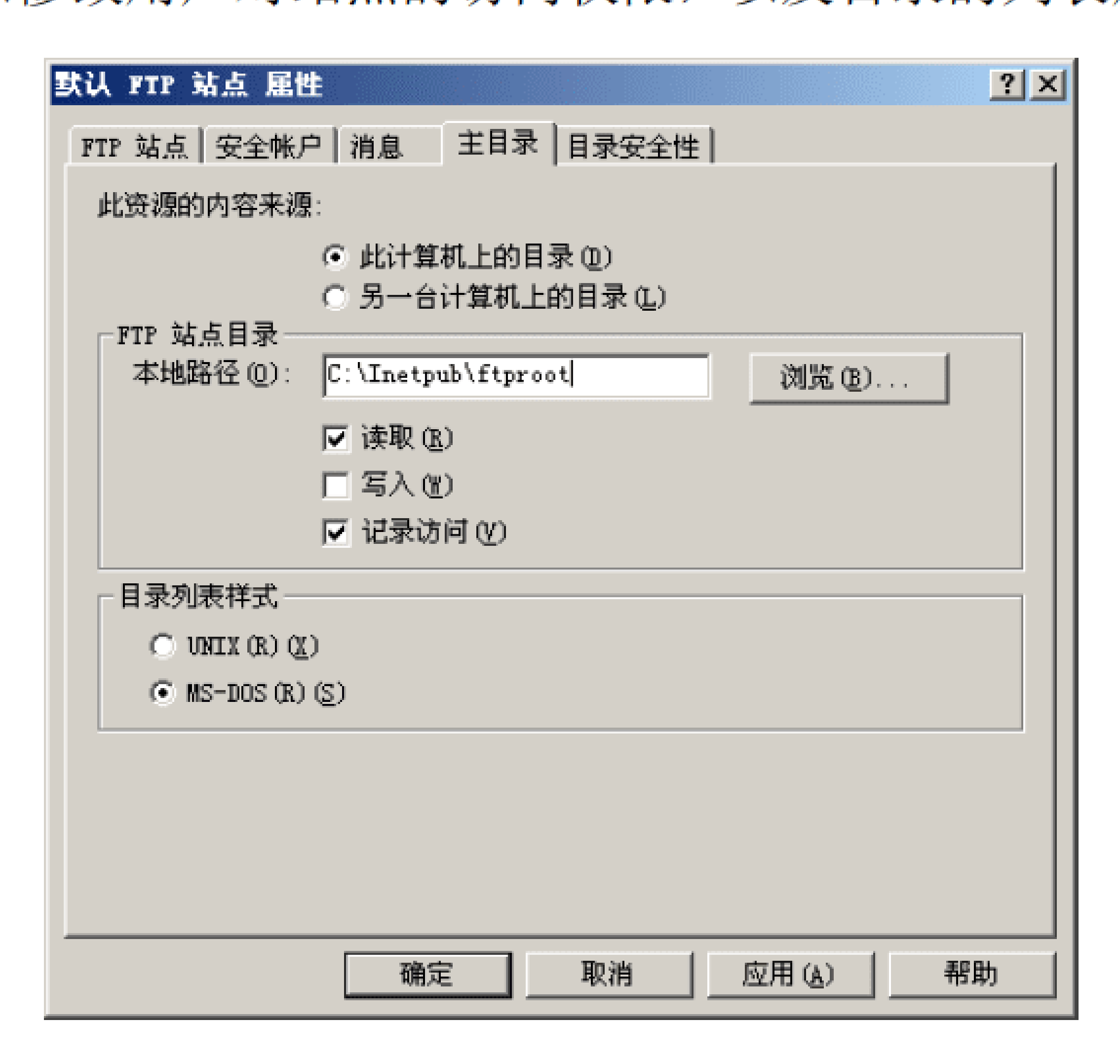


图 2-45 【主目录】选项卡

4) 访问安全设置

FTP 站点的安全非常重要，Windows Server 2003 中对 FTP 服务器可配置用户身份认证、限制访问 FTP 的 IP 地址，从而确保站点的安全。

(1) 禁止匿名访问。禁止匿名访问在属性信息的【安全帐户】选项卡中设置。在默认情况下，FTP 站点允许用户匿名访问，如果站点安全性要求较高，取消选中【允许匿名连接】复选框即可禁止用户匿名访问该 FTP 站点，如图 2-46 所示。

(2) 限制 IP 地址。限制 IP 地址在 FTP 站点属性的【目录安全性】选项卡中设置。通过对 IP 地址的限制可以只允许某些特定的计算机访问该站点，从而避免外界恶意攻击，如图 2-47 所示。有两种方式来限制 IP 地址的访问：一是【授权访问】，其含义是除列表中 IP 地址的主机不能访问外，其他所有主机都可以访问该 FTP 站点，主要用于给 FTP 服务器加入“黑名单”；二是【拒绝访问】，其含义是除列表中 IP 地址的主机能访问外，其他所有主机都不能访问该 FTP 站点，主要用于内部 FTP，以防止外部主机访问该 FTP 站点。

5) 设置消息

消息主要是指在用户登录或退出时显示的信息。可在 FTP 站点属性的【消息】选项卡中设置，如图 2-48 所示。在【欢迎】文本框中输入用户登录时显示的信息，在【退出】文本框中输入用户退出时显示的信息。在此选项卡中可以设置当超过最大连接人数时，给提出连接请求的客户机发送一条报错信息，若要设置此功能就在【最大连接数】文本框中输入报错信息。

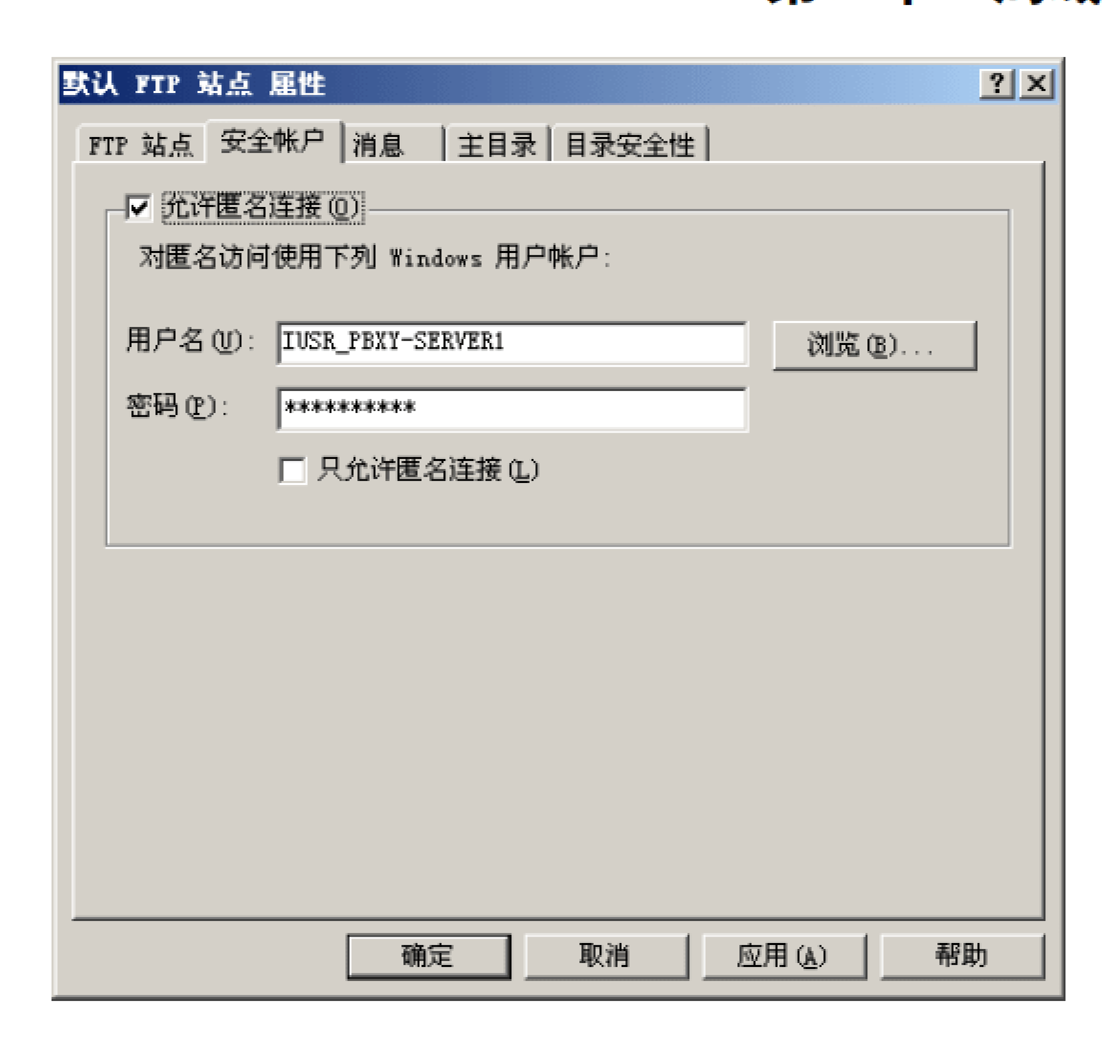


图 2-46　【安全帐户】选项卡

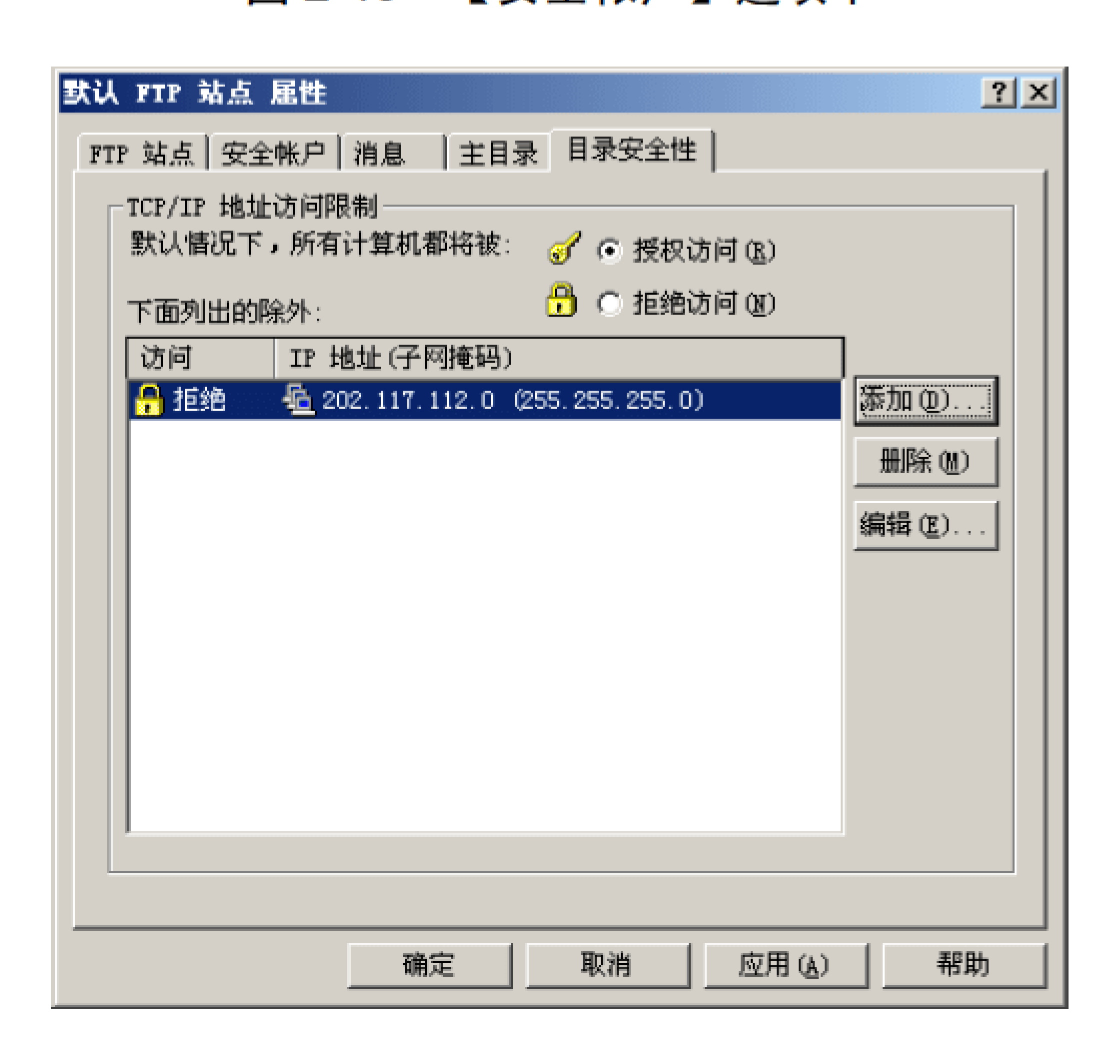


图 2-47　【目录安全性】选项卡



图 2-48　【消息】选项卡

6) 建立虚拟目录

当有个目录需要通过 FTP 站点进行发布，而又不是存放在主目录之下的目录时，称此目录为 FTP 虚拟目录。

建立虚拟目录的步骤如下。

(1) 右击 FTP 站点，在弹出的快捷菜单中选择【新建】|【虚拟目录】命令，打开【虚拟目录创建向导】对话框。

(2) 在【虚拟目录别名】界面中，输入虚拟目录别名(访问时用的名字)，单击【下一步】按钮，如图 2-49 所示。

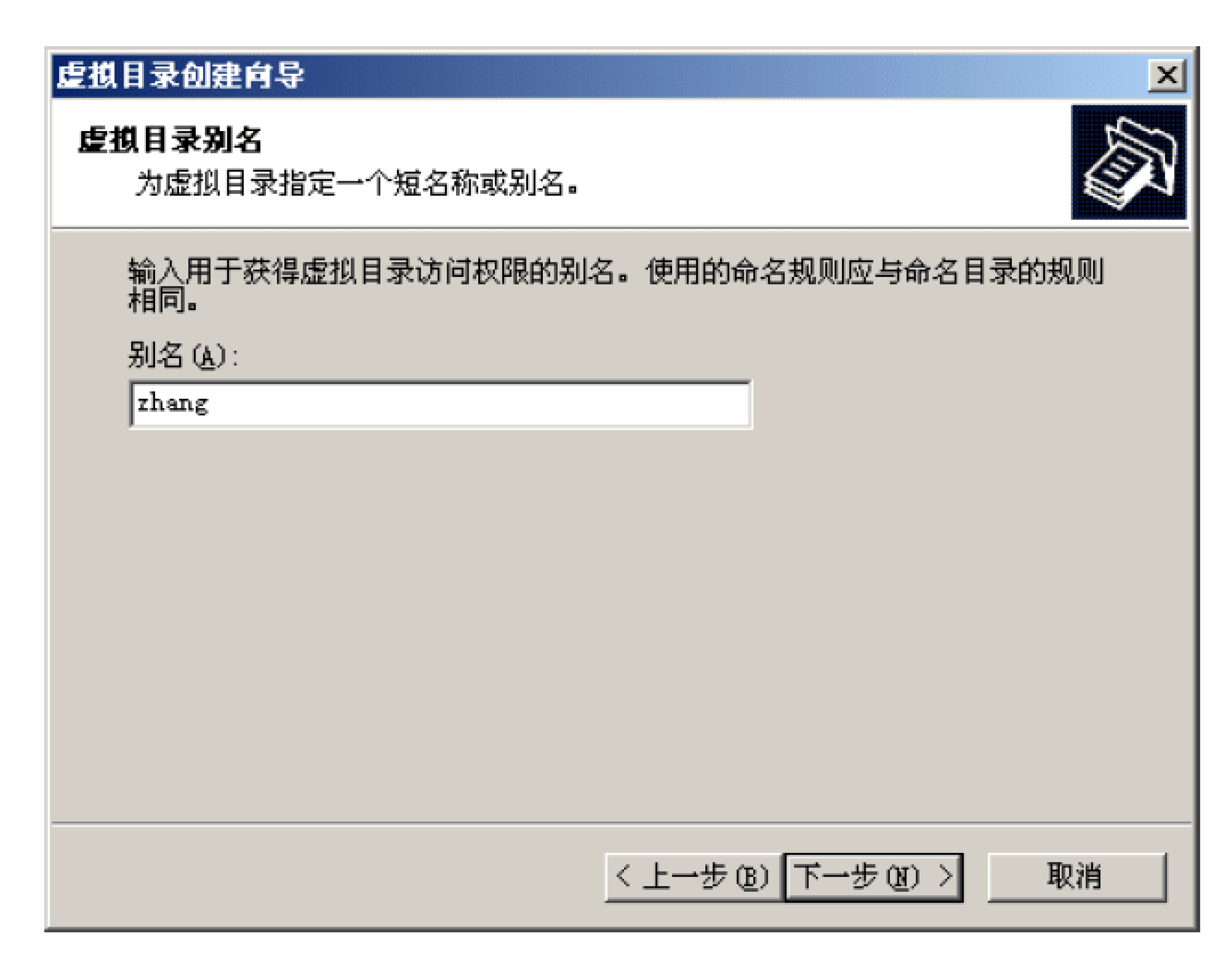


图 2-49 【虚拟目录别名】界面

(3) 在【FTP 站点内容目录】界面中，输入虚拟目录所映射的真实路径，单击【下一步】按钮，如图 2-50 所示。

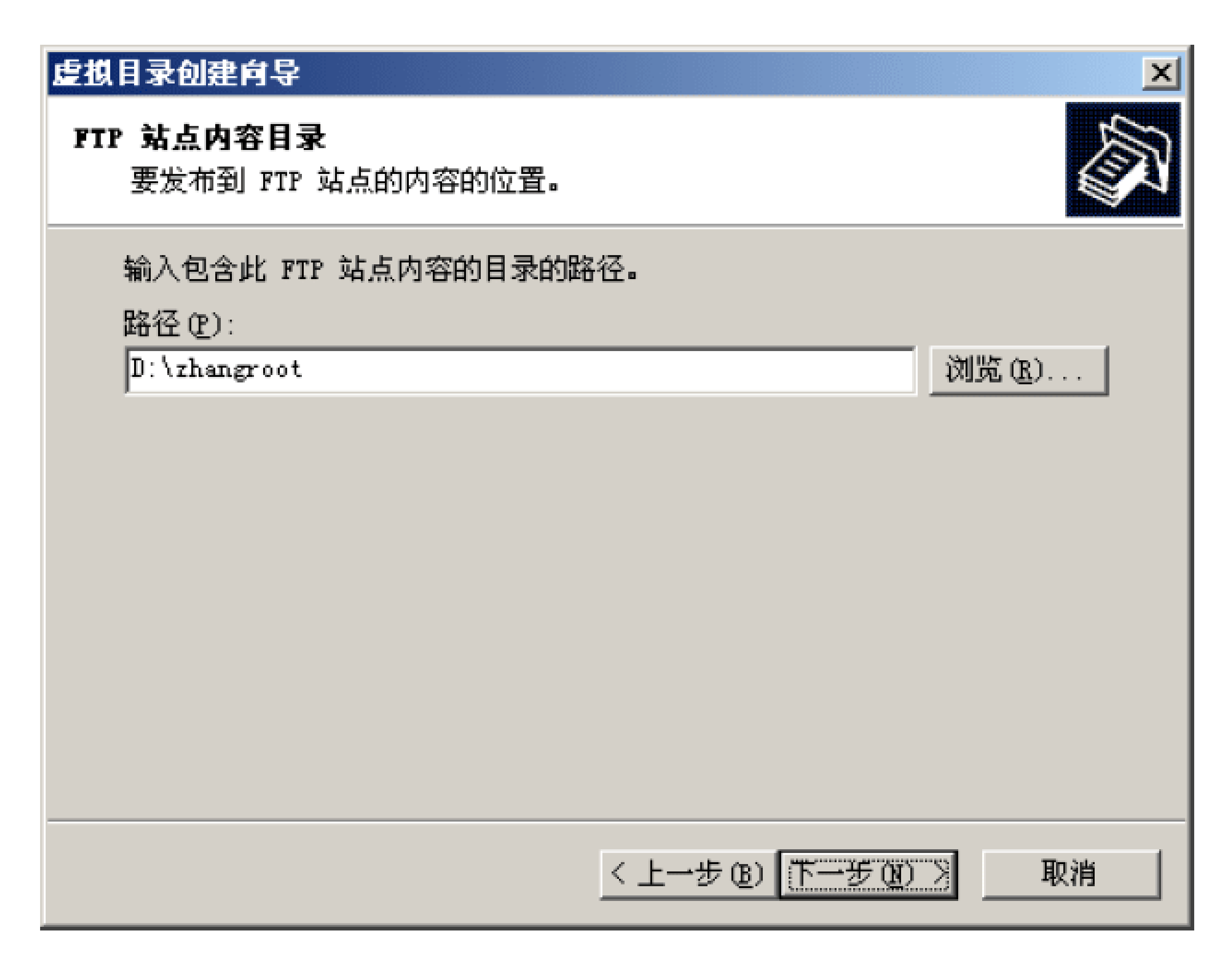


图 2-50 【FTP 站点内容目录】界面

(4) 在【虚拟目录访问权限】界面中，设置该目录的访问权限。可选中【读取】复选

框，也可以选中【写入】复选框。单击【下一步】按钮即可完成虚拟目录的建立，如图 2-51 所示。

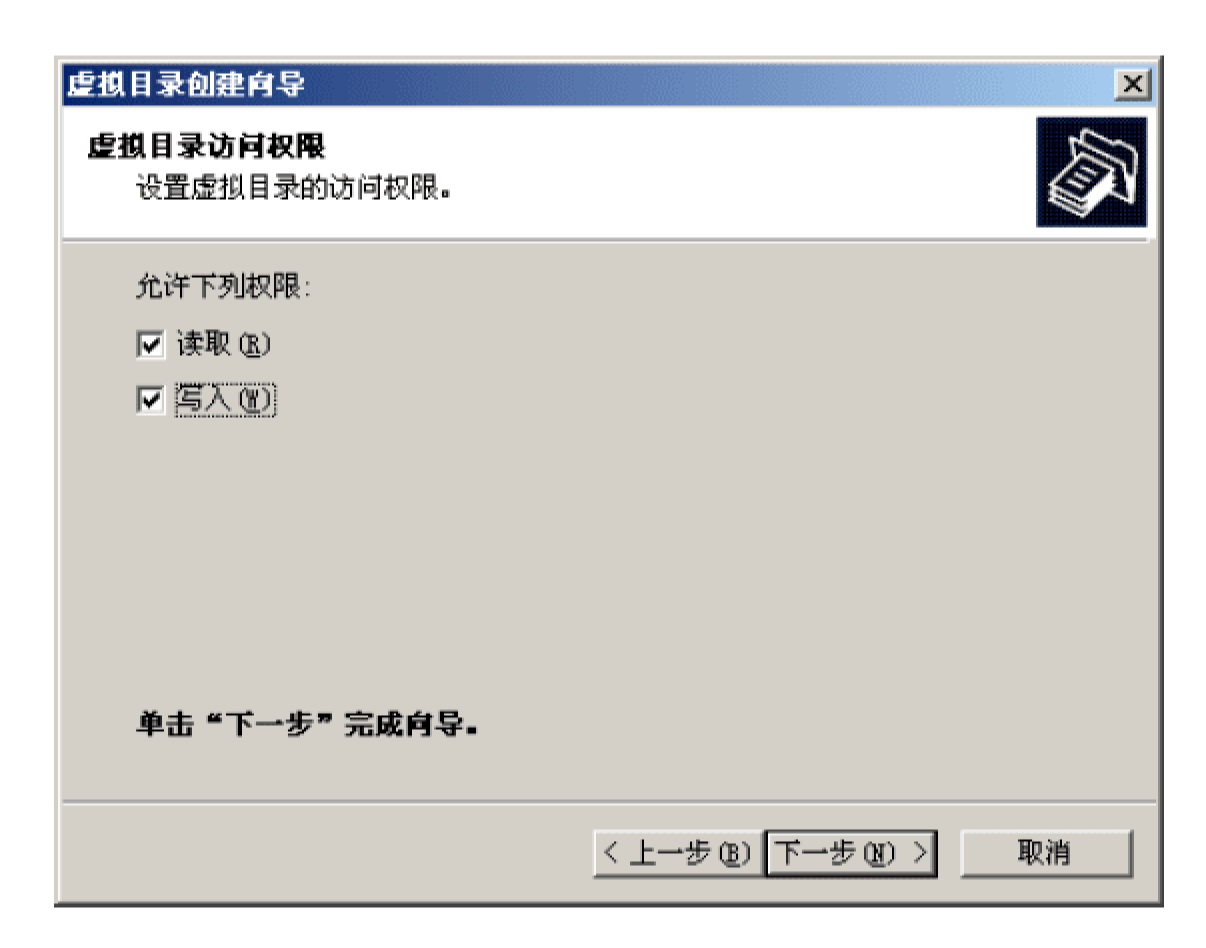


图 2-51　【虚拟目录访问权限】界面

虚拟目录与真实目录一样，也可以为其设置安全性和访问控制，默认情况下都继承站点的安全性和访问控制。用户可自行修改，修改方法同上。

这里要注意的是，当一个注册用户登录到 FTP 站点时，若有和该用户帐号同名的真实目录和虚拟目录时，将自动进入该目录。

2.4.1.2　Linux 下 Wu-FTP 服务器的安装与配置

在 Linux 环境下使用的 FTP 服务器软件主要有 Wu-FTP、NcFTP 和 ProFTP 三种。由于 Wu-FTP 是目前最流行的一种免费 FTP 服务器软件，所以下面主要介绍 Wu-FTP。

1. Wu-FTP 功能和特征

1) Wu-FTP 的特征

- Wu-FTP 是基于 GPL 协议开发的，它是一个源码公开的自由软件。
- Wu-FTP 是历史最久的非商业 FTP 服务器程序之一，它的影响非常广泛。
- Wu-FTP 项目仍然继续进行，新的特性不断被加入。
- Wu-FTP 支持广泛的 UNIX 和类 UNIX 平台。

2) Wu-FTP 的功能

- 可以控制不同网络和域的用户对 FTP 服务器的存取权限和访问时段。
- 使用者在下载文件时，可以自动对其进行压缩和解压缩工作。
- 可以记录文件上传和下载的全过程。
- 可以显示传输时的相关信息，方便用户及时了解目前的传输动态。
- 可以设置最大连接数，从而提高了效率，且有效地控制了负载。
- 可以暂时关闭 FTP 服务器，以便系统维护。

2. Wu-FTP 服务器的获取与安装

Wu-FTP 有 RPM 包分发版本，可以从 Red Hat 网站下载或在 Red Hat 7.0 的光盘中找到。二进制的分发版本可以从 ftp：//ftp.wu-ftpd.org/pub/wuftpd 处进行下载。

下面以 RPM 的安装为例介绍 Wu-FTP 的安装过程。

若在安装 Red Hat 时没有安装 Wu-FTP，则可以使用下面的命令进行安装：

```
#rpm -ivh wu-ftpd-2.6.0.i386.rpm
```

若获得了更新版本的 Wu-FTP 的 RPM，可以使用下面的命令进行升级：

```
#rpm -Uvh wu-ftpd-2.6.x.i386.rpm
```

当安装完成后，系统中将存在如表 2-6 所示的文件。

表 2-6　Wu-FTP 的主要文件

类　型	文 件 名	说　明
可执行文件	/usr/bin/ftpcount	显示目前在线人数
	/usr/bin/ftpwho	查看目前 FTP 服务器的连接情况
	/usr/sbin/ckconfig	检查设置是否正确
	/usr/sbin/ftprestart	重新启动 FTP 服务器
	/usr/sbin/ftpshut	用于关闭服务程序
	/usr/sbin/in.wuftpd	FTP 服务程序
	/usr/sbin/privatepw	改变 Wu-FTP 组访问文件
配置文件	/etc/ftpaccess	Wu-FTP 的主配置文件，控制存取权限
	/etc/ftpconversions	用来控制当传输文件的时候是否进行压缩
	/etc/ftpusers	禁止某些用户登录
	/etc/ftphosts	禁止某些来自指定机器上的登录
	/etc/ftpgroups	创建用户组，这个组中的成员预先定义可以访问 FTP 服务器
手册	/usr/share/doc/wu-ftpd-2.6.1/	存放 Wu-FTP 手册页
文档	/usr/share/man/	存放 Wu-FTP 文档

3. *启动* Wu-FTP

1)　修改/etc/services

需要确定/etc/services 文件有以下一行内容，同时该内容未被加上注释符“#”：

```
ftp          21/ftp       ftp
```

2)　创建/etc/xinetd.d/wu-ftpd 文件

文件大致内容如下：

```
service ftp
{
disable                 = no
socket_type             = stream
wait                    = no
user                    = root
server                  = /usr/sbin/in.ftpd
```

```
server_args          = -l -a
log_on_success       += DURATION USERID
log_on_failure       += USERID
nice                 =10
}
```

3)　重新启动 xinetd

要想使修改内容立即生效，可以重新启动 xinetd 程序。其命令是：

```
#/etc/rc.d/init.d/xinetd restart
```

4)　测试 Wu-FTP 是否启动

与测试 Sendmail 服务器一样，可以通过 telnet 命令登录到 21 端口来测试 Wu-FTP 服务是否启动。其命令是：

```
#telnet localhost 21
```

如果登录成功，则表明该服务器已成功安装并启动。

4.　Wu-FTP 服务器的配置

1)　/etc/ftpuser 的配置

/etc/ftpuser 用来指定某些用户不能登录本 FTP 服务器。其实这个设置是十分简单的，只需将要禁止的用户帐号写入文件/etc/ftpuser 中。由于从系统的安全考虑，一般我们不希望权限过大的用户和一些与命令名相同的用户进入 FTP 服务器，所以在默认的配置中，一般来说以下用户已经被列入了“黑名单”。

```
root
uucp
news
bin
adm
nobody
lp
sync
shutdown
halt
mail
```

2)　/etc/ftphosts 的配置

/etc/ftphosts 用来指定某些主机不能连接本 FTP 服务器。要禁止某些来自指定机器上的登录可以有两种方法：一种是在/etc/ftpaccess 中设置 deny 命令，另一种是在/etc/ftphosts 中写入要禁止的主机的 IP 地址或域名。下面是一个/etc/ftphosts 文件的范例：

```
allow xyz *.abc.com.cn 210.102.0.0/16
deny tom *.hanker.com 131.222.154.0/24
```

例中允许用户 xyz 从域名以 abc.com.cn 为后缀的主机及 210.102.0.0/255.255.0.0 的主机上登录；禁止用户 Tom 从域名 hanker.com 为后缀的主机及 131.222.154.0/255.255.255.0 的主机上登录。当用户名为 anonymous 或 ftp 时，均表示匿名用户。

3)　/etc/ftpconversions 的配置

/etc/ftpconversions 文件主要定义用户从 FTP 服务器中下载文件时对文件进行格式转换的规则，如压缩、解压缩、打包和开包等操作。这样用户就不必为.tar.gz、.tgz、.Z、.z 之类的文件伤脑筋了。

/etc/ftpconversions 文件的格式乍看上去很复杂，不过不必担心，基本上不用修改、设置。下面是一个/etc/ftpconversions 文件，它已经能够满足一般的使用需要了。

```
:.Z: : :/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
: : :.Z:/bin/compress -c %s:T_REG:O_COMPRESS:COMPRESS
:.gz: : :/bin/gzip -cd %s:T_REG|T_ASCII:O_UNCOMPRESS:GUNZIP
: : :.gz:/bin/gzip -9 -c %s:T_REG:O_COMPRESS:GZIP
: : :.tar:/bin/tar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
: : :.tar.Z:/bin/tar -c -Z -f - s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+COMPRESS
: : :.tar.gz:/bin/tar -c -z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+GZIP
```

如果想让 FTP 服务器有自动压缩、解压缩的功能，必须先将一些压缩、解压缩的命令文件如 tar、gzip、gunzip、compress、uncompress 等命令文件复制到/home/ftpd/bin 目录下。

4)　/etc/ftpaccess 的配置

/etc/ftpaccess 是 FTP 服务器上最重要的配置文件，它主要控制 FTP 存取权限，直接关系到 FTP 服务器能否正常工作，还有其他许多权限上的设置。下面是一个典型的配置实例。

```
loginfails 3
class local real *
class remote anonymous guest *
limit remote 100 Any /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check rfc822 warn
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
delete no anonymous,guest
overwrite no anonymous,guest
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias inc /incoming
email guest@xxx.net
email guest@yyy.net
deny *.com.tw /etc/ftpd/deny.msg
```

下面逐条进行讲解，并给出每条设置的含义，以便读者触类旁通，根据自己 FTP 服务器的具体情况进行合理设置。

- 登录重试次数

  格式：loginfails [次数]

  功能：设置当用户登录到 FTP 服务器时，允许用户输入错密码的次数。

  实例：loginfails 3，密码输入错误 3 次就切断连接。

- 定义用户类别

  格式：class [类名] [real/guest/anonymous] [IP 地址]

  功能：用于设置 FTP 服务器上用户的类别，并可对客户端的 IP 地址进行限制，允许某部分的 IP 地址或全部的 IP 地址访问。而在 FTP 服务器上的用户基本上可以分为以下 3 类。

  ① real：在该 FTP 服务器有合法帐号的用户。

  ② guest：有记录的匿名用户。

  ③ anonymous：权限最低的匿名用户。实例：class local real *：定义一个名为 local 的类，它包括在任何地方登录(*代表所有 IP 地址)的 real 用户。

  class remote anonymous guest *：定义一个名为 remote 的类，它包括在任何地方登录的 anonymous 用户和 guest 用户。

- 登录人数的限制

  格式：limit [类别] [人数] [时间] [文件名]

  功能：设置指定时间内指定的类别允许连接的人数上限。当达到人数上限的时候，显示指定文件的内容。

  实例：limit remote 100 Any/etc/ftpd/toomany.msg　在任何时间内，remote 类的访问用户达到 100 人时，将不再允许或无法产生新的连接。当第 101 位用户要连接时，连接将失败，并向用户出示文件/etc/ftpd/toomany.msg 的内容。

- 用户登录时显示的文件

  格式：message [文件名称] [指令]

  功能：当用户执行指定的指令时，系统将指定的文件内容显示出来。

  实例：message/etc/ftpd/welcome.msg login　当用户执行 login 命令时，也就是登录到 FTP 服务器上的时候，系统将显示文件/etc/ftpd/welcome.msg 的内容。

- 压缩功能

  格式：compress [yes/no] [类别]

  功能：设置某个类别的用户可以使用 compress(压缩)功能。

  实例：compress yes local remote　允许 local 和 remote 两类用户都能使用 compress(压缩)功能。

- 归档功能

  格式：tar [yes/no] [类别]

  功能：设置某个类别的用户可以使用 tar(归档)功能。

  实例：tar yes local remote　允许 local 和 remote 两类用户都能使用 tar 功能。

- 是否支持群组

  格式：private [yes/no]

  功能：设置是否支持群组对文件的取用。

  实例：private yes　支持群组对文件的取用。

- 匿名用户密码检查

  格式：passwd-check [none/trivial/rfc822] [enforce/warn]

  功能：设置匿名用户 anonymous 的密码使用方式。

  none 表示不作密码验证，任何密码都可以登录。

  trival 表示只要输入的密码中含有字符“@”就可以登录。

  rfc822 表示密码一定要符合 RFC 822 中所规定的 E-mail 地址才能登录。

  enforce 表示输入的密码不符合以上指定的格式就不允许登录。

  warn 表示密码不符合规定时只出现警告信息，仍然能够登录。

  实例：passwd-check rfc822 warn　希望能够得到符合规定的 E-mail 作为密码，但如果不是，也允许登录。

- 操作日志

  格式：log command [real/guest/anonymous]

  功能：设置某些用户登录后的操作记录在文件/usr/adm/xferlog 中。

  实例：log command real　当 real 用户登录后，将其操作记录下来。由于其他用户权限较低，所以操作不会引起太大的安全隐患，所以一般只需记下 real 用户的操作就可以了。

- 文件传送日志

  格式：log transfer [real/guest/anonymous] [inbound/outbound]

  功能：设置某些用户的上传(Inbound)和下载(Outbound)操作日志。

  实例：log transfer anonymous guest inbound outbound　对于匿名用户要更加关注他们的文件操作，所以无论上传、下载都进行记录。

  log transfer real inbound：对于合法用户则只记录他的上传记录。

- FTP 服务器关闭设置文件

  格式：shutdown [文件名]

  功能：FTP 服务器关闭的时间可以设置在后面所指定的文件中，当设置的时间一到，便无法登录 FTP 服务器了，要恢复的话，只有将这个文件删掉。而这个文件必须由指令/bin/ftpshut 来生成。

  实例：shutdown /etc/ftpd/shut.msg

- 删除文件权限设置

  格式：delete [yes/no] [real/anonymous/guest]

  功能：设置是否允许指定用户使用 delete 命令删除文件。默认是允许。

  实例：delete no anonymous,guest　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 delete 命令。

- 覆盖文件权限设置

  格式：overwrite [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户覆盖同名文件。默认是允许。

实例：overwrite no anonymous,guest　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户覆盖同名文件。

- 文件改名权限设置

格式：rename [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 rename 命令来为文件改名。默认是允许。

实例：rename no anonymous　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 rename 命令改变文件名。而对有记录的匿名用户则适当地放宽，允许他们使用改名命令。

- chmod 命令权限设置

格式：chmod [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 chmod 命令更改文件权限。默认是允许。

实例：chmod no anonymous, guest　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 chmod 命令更改文件权限。

- umask 命令权限

格式：umask [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 umask 命令。默认是允许。

实例：umask no anonymous　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 umask 命令。

- 用户上载目录

格式：upload [根目录] [上传目录] [yes/no] [用户] [权限] [dirs/nodirs]

功能：对可以上传的目录进行更加详细的设置。

实例：upload /home/ftpd * no　表示在子目录/home/ftpd 下不允许上传。

upload /home/ftpd /bin no　表示在子目录/home/ftpd/bin 下不允许上传。

upload /home/ftpd /etc no　表示在子目录/home/ftpd/etc 下不允许上传。

upload/home/ftpd/pub yes real 0644 dirs　允许服务器上的合法用户在子目录/home /ftpd/pub 下可以上传权限为 0644(也就是-rw-r--r--)的文件，而且在这个目录下可以新建子目录。

upload /home/ftpd /incoming yes real guest anonymous 0644 dirs　允许所有的用户在子目录/home/ftpd/incoming 下可以上传权限为 0644 的文件，而且在这个目录下可以新建子目录。

- 虚拟目录

格式：alias [目录别名] [目录名]

功能：为指定目录设置一个别名，在切换目录时就可以使用较短的目录别名。

实例：alias inc：/incoming　为子目录 incoming 设置一个别名 inc。

- 管理员的 E-mail 地址

格式：email [guest 的 E-mail 地址]

功能：只要在此设置系统管理员的 E-mail 地址，FTP 服务器有问题或任何信息都要通知系统管理员。

实例：email guest@XXX.net 这里仅是一个示例，实际上可以包含多个符合规范的 E-mail 地址。

● 访问限制

格式：deny [IP 地址/域名] [说明文件]

功能：可以限制某些 IP 地址或域名的用户无法登录 FTP 服务器。

实例：deny *.com.tw/etc/ftpd/deny.msg 设置凡是以.com.tw 结束的域名，都禁止其访问。而将/etc/ftpd/deny.msg 的内容显示给用户看。

5. 与 Wu-FTP 相关的其他一些命令的使用

1) 连接数字统计命令 ftpcount

使用 ftpcount 命令可以十分清楚地统计出当前连接到 FTP 服务器上的用户数，并且同时列出上限。命令输出如下所示：

```
#ftpcount
Service class local    -   0   users   (20     maximum)
Service class remote   -   5   users   (100    maximum)
```

上例中显示属于 local(本地)的有 0 个人在线，上限为 20；属于 remote(远程)的有 5 个人在线，上限为 100。

2) 在线用户查看命令 ftpwho

使用 ftpwho 命令可以查看当前连接的用户的详细情况。命令输入如下所示：

```
#ftpwho
Service class all:
ftp     12586   536 0   21:58 ? 00:00:00 ftpd: abc.com.cn :anonymous
ma      12557   532 0   21:58 ? 00:00:00 ftpd: localhost:ma:IDLE
-2  users (no maximum)
```

上例中显示 all 类有两个用户登录，并显示登录时间、来源和状态。

3) FTP 关闭文件生成命令 ftpshut

可以使用 ftpshut 命令生成一个在目录/etc/ftpaccess 中设置的 shut.msg 文件，用于关机设定。ftpshut 命令的格式为

```
#ftpshut [-l<分钟>][-d<分钟>] [关闭时间]  ["警告信息"]
```

● -l<分钟>：指定在关闭 FTP 服务器功能前多少分钟时停止用户的连接。

● -d<分钟>：指定在关闭 FTP 服务器功能前多少分钟时切断用户连接。

● 关闭时间：指定关闭 FTP 服务器的时间。例如，6:20 则写为 0620。如果要立即关闭，可以用 now。

● "警告信息"：指定断线之前显示给用户的警告信息。

下面是 ftpshut 运行实例：

```
#ftpshut -l25 -d5 2300 "Warn: FTP server will shutdown!"
#cat /etc/shutmsg
2001    18  23  00  0025    0005
Warn:FTP server will shutdown!
```

例子中的 FTP 服务器将在 23：00 关闭，关闭前 25 分钟将拒绝用户登录，关闭前 5 分钟将断开所有连接，并给在线用户发送 Warn:FTP server will shutdown!消息。

如果要立即关闭 FTP 服务器，则输入：

```
#ftpshut now
```

FTP 服务器关闭后要重新启动，只要把目录/etc/shutmsg 下的这个文件删除，并重新启动 FTP 服务器就可以继续 FTP 服务了。

2.4.2　典型例题分析

例 1　阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2009 年 11 月下午试题二)

【说明】

某公司要在 Windows 2003 Server 上搭建内部 FTP 服务器，服务器分配有一个静态的公网 IP 地址 228.121.12.38。FTP 服务器的创建可分为安装、配置、测试三个过程。其中图 2-52 和图 2-53 分别为配置过程中 FTP 站点创建和 FTP 站点属性的配置窗口。

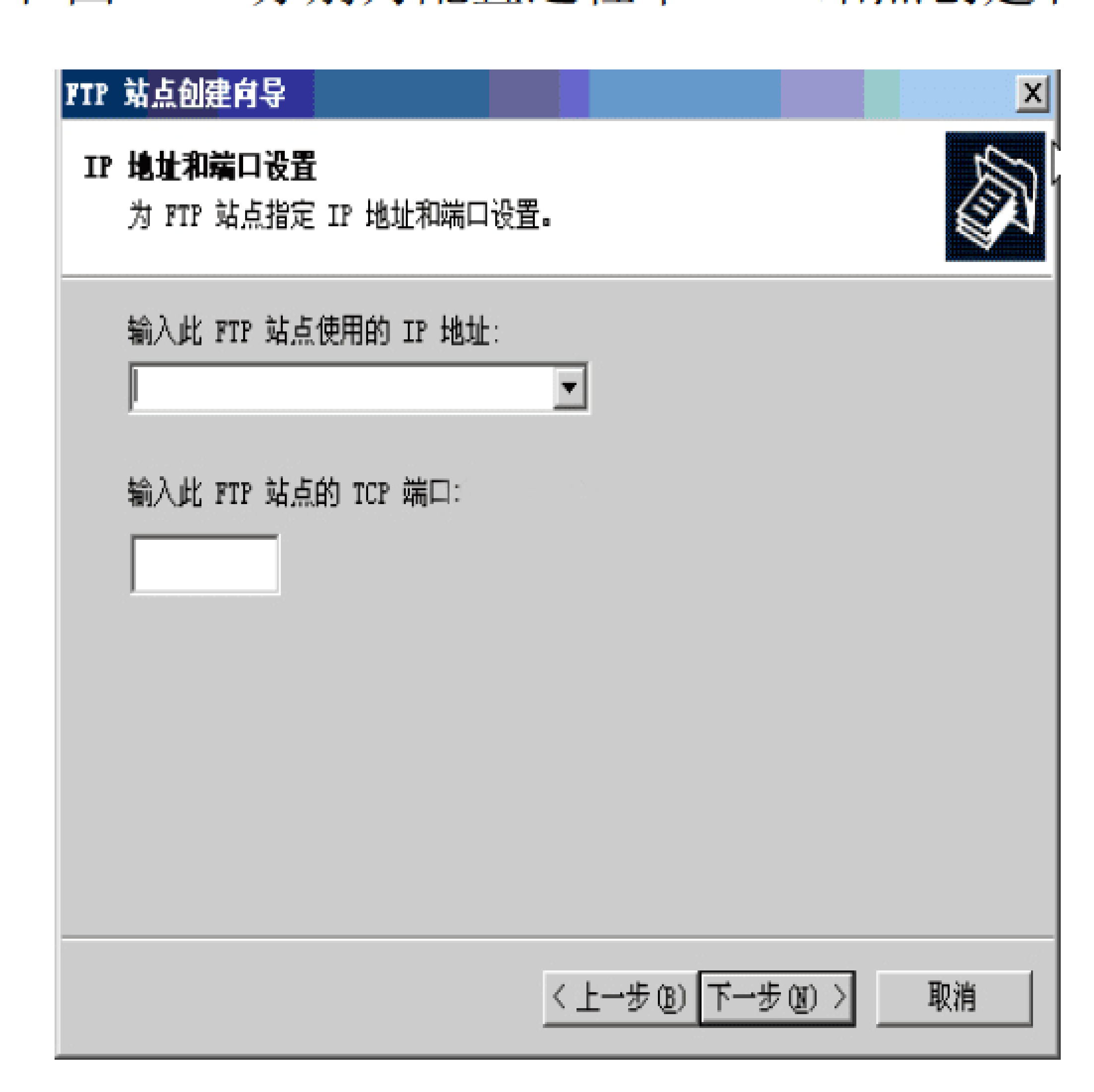


图 2-52　【IP 地址和端口设置】对话框

默认 FTP 站点 属性
FTP 站点 | 安全帐户 | 消息 | 主目录 | 目录安全性
此资源的内容来源:
此计算机上的目录(D)
另一台计算机上的目录(L)
FTP 站点目录
本地路径(O):
浏览(B)...
读取(R)
写入(W)
记录访问(V)
目录列表样式
UNIX (R) (X)
MS-DOS (R) (S)
确定　取消　应用(A)　帮助

图 2-53　【主目录】选项卡

【问题 1】(2 分)

在 Windows 2003 中安装 FTP 服务，需在【应用程序服务器】选项的__(1)__组件复选框中选择【文件传输协议(FTP)服务】进行安装。

A．ASP.NET　　　　B．Internet 信息服务(IIS)

C．应用程序服务器控制台　　　　D．启用网络服务

【问题 2】(4 分)

在图 2-52 中，在【输入此 FTP 站点使用的 IP 地址】文本框中应填入__(2)__，默认情况下【输入此 FTP 站点的 TCP 端口】文本框中应填入__(3)__。

【问题3】(2分)

在图2-53中，如果FTP资源存储在F盘，新建FTP站点的默认主目录为__(4)__。

A．F:\inetpub\ftproot　　B．F:\ftp

C．F:\ftp\root　　D．F:\inetpub\wwwroot

【问题4】(4分)

FTP服务器配置完成后，可以在网络上另一台PC中测试FTP是否配置成功。测试过程为：在该计算机上命令行模式下输入命令__(5)__(填空)，在出现USER提示时输入FTP服务器上计算机管理员名称和密码就可以登录了。如果该FTP上开启了匿名访问功能，在用户名处输入__(6)__，密码处填写一个E-mail地址也可以登录。

A．anonymous　　B．user　　C．administrator

【问题5】(3分)

依据图2-53的配置，该FTP服务器配置完成后，用户可以上传文件吗？为什么？

分析：

在Windows Server 2003系统中配置FTP服务器的步骤如下。

① 依次选择【开始】|【管理工具】|【Internet信息服务(IIS)管理器】命令，打开【Internet信息服务(IIS)管理器】窗口。在左侧窗格中展开【FTP站点】目录，右击【默认FTP站点】选项，在弹出的快捷菜单中选择【属性】命令。

② 打开【默认FTP站点 属性】对话框，在【FTP站点】选项卡中可以设置关于FTP站点的参数。其中，在【FTP站点标识】区域中可以更改FTP站点名称、监听IP地址以及TCP端口号，单击【IP地址】文本框右侧的下三角按钮，并选中该站点要绑定的IP地址。

③ 切换到【安全帐户】选项卡，此选项卡用于设置FTP服务器允许的登录方式。默认情况下允许匿名登录，如果取消选中【允许匿名连接】复选框，则用户在登录FTP站点时需要输入合法的用户名和密码。

④ 切换到【消息】选项卡，在【标题】文本框中输入能够反映FTP站点属性的文字，该标题会在用户登录之前显示。

⑤ 切换到【主目录】选项卡。主目录是FTP站点的根目录，当用户连接到FTP站点时只能访问主目录及其子目录的内容，而主目录以外的内容是不能被用户访问的。主目录既可以是本地计算机磁盘上的目录，也可以是网络中的共享目录。

⑥ 切换到【目录安全性】选项卡，在该选项卡中主要用于授权或拒绝特定的IP地址连接到FTP站点。

⑦ 返回【默认FTP站点属性】对话框，单击【确定】按钮使设置生效。

【问题1】

由步骤①可知，(1)的答案为B。

【问题2】

由题目可知，公网IP地址为228.121.12.38，故(2)的答案为228.121.12.38。TCP端口，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。常见的包括FTP服务的21端口，Telnet服务的23端口，SMTP服务的25端口，以及HTTP服务的80端口等。故(3)的答案为21。

【问题 3】

完成上述步骤①～步骤⑦后，FTP 服务器已配置为接受传入的 FTP 请求。将要提供的文件复制或移动到 FTP 发布文件夹以供访问。默认的文件夹是驱动器：\inetpub\ftproot，其中驱动器是安装 IIS 的驱动器。故(4)选 A。

【问题 4】

登录 FTP 可以直接在 ftp 的提示符下输入“open 主机 IP ftp 端口”，然后按 Enter 键。一般端口默认都是 21，可以不写。然后输入合法的用户名和密码。故(5)的答案为 open 228.121.12.38。

登录 FTP 服务器的方式可以分为两种类型：匿名登录和用户登录。如果采用匿名登录，则用户可以通过用户名 anonymous 连接到 FTP 服务器，以电子邮件地址作为密码。对于这种密码，FTP 服务器并不进行检查，只是为了显示方便才进行这样的设置。故(6)选 A。

【问题 5】

在步骤⑤时，可以根据实际需要选中或取消选中【写入】复选框，以确定用户是否能够在 FTP 站点中写入数据。由图 2-53 可知，【写入】复选框未选中，故该 FTP 站点相应目录不允许上传文件。

答案：

【问题 1】

(1) B

【问题 2】

(2) 228.121.12.38

(3) 21

【问题 3】

(4) A

【问题 4】

(5) open 228.121.12.38

(6) A

【问题 5】

不可以。因为未选中【写入】复选框，该 FTP 站点相应目录不允许上传文件。

例 2　阅读以下说明，回答问题 1～问题 3，将解答填入答题纸对应的解答栏内。(2007 年 11 月下午试题三)

【说明】

应用 FTP 在两台计算机之间传输文件，一台计算机作为 FTP 客户端，安装 FTP 客户端软件(或操作系统自带)；另一台作为 FTP 服务器，安装 FTP 服务端软件(如 vsftp)。

【问题 1】(4 分，其中空(2)2 分，空(1)、空(3)各 1 分)

FTP 协议属于 TCP/IP 模型中的__(1)__协议，基于 TCP 协议在客户端和服务器之间传送所有数据，TCP 是一个__(2)__的协议。其主要特点是__(3)__，这对于文件传输而言是非常重要的。

其中(1)、(2)备选答案：

(1)　A．应用层　　B．传输层　　C．网络层　　D．物理层

(2) A．无连接　　B．面向连接

【问题2】(4分)

FTP服务器有两个保留的端口号。在默认情况下，端口__(4)__用于发送和接收FTP的控制信息，端口__(5)__用于发送和接收FTP数据。

FTP客户端与FTP服务器建立连接时，系统为其自动分配一个端口号，可选择的范围是__(6)__～__(7)__。

【问题3】(7分)(空(10)2分，其他每空1分)

(8)是Linux系统的守护进程，而vsftp不是守护进程管辖下的服务，可采用下面的命令启动vsftp服务：

```
/etc/rc.d/init.d/vsftpd (9)
```

vsftp的配置文件是/etc/vsftpd/vsftpd.conf，该文件有很多配置项，其中：

anonymous_enable=[YES]，允许以__(10)__模式登录ftp服务器。

local_umask=022，指定了访问权限。如果用户建立一个目录，则同组用户对该目录的访问权限是__(11)__。

vsftp的默认访问目录是__(12)__，客户端可在这个目录下上传、下载文件。

除了专用ftp客户端程序外，不能用来访问ftp服务器的是__(13)__。

其中(8)、(12)、(13)空的填写内容在以下候选答案中选择：

(8) A．xinetd　　B．service　　C．admin

(12) A．/etc/ftp　　B．/var/ftp　　C．/usr/ftp

(13) A．DOS命令行　　B．IE浏览器　　C．outlook

分析：本题考查FTP的应用和Linux下FTP的有关配置。

FTP是Internet最古老的协议之一，应用于TCP/IP网络上的文件传输。要使用FTP在两台计算机之间传输文件，一台计算机必须是FTP客户端，而另一台则必须是FTP服务器。FTP会话建立并传输文件的过程如下。

① 为了建立一个TCP连接，客户端和服务器必须打开一个TCP端口。FTP服务器有两个预分配端口号：21和20。其中端口21用于发送和接收FTP的控制信息。FTP服务器连接监听这个端口，以监听请求连接到服务器的FTP客户。一个FTP会话建立后，端口21的连接会在会话期间始终保持打开状态。端口20用于发送和接收FTP数据。该数据端口只在传输数据时打开，并在传输结束时关闭。

② FTP客户端程序在激发FTP客户端服务后，可动态分配其端口号，可选择的范围为1024～65 535。

③ 当一个FTP会话开始后，客户端程序打开一个控制端口，该端口连接到服务器上的端口21上。

④ 需要传输数据时，客户端再打开连接到服务器端口20的第二个端口，每当开始传输文件时，客户端程序都会打开一个新的数据端口，在文件传输完毕后，再将该端口自动关闭。

FTP使用TCP协议在客户端和服务器端之间传送所有通信和数据。TCP是一个面向连接的协议，也就是说，在传输数据前，需要在客户端和服务器之间建立通信会话，而且在

整个 FTP 会话期间，该连接将一直保持。面向连接会话的主要特点是其可靠性和错误恢复能力，而对于文件传输而言，是非常重要的。

答案：

【问题 1】

(1)　A　　(2)　B　　(3)　可靠性

【问题 2】

(4)　21　　(5)　20

(6)　1024　　(7)　65 535

【问题 3】

(8)　A　　(9)　start

(10) 匿名用户　　(11) 5 或可读可执行

(12) B　　(13) C

例 3　请认真阅读下面的说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题三)

【说明】

某单位使用 IIS 建立了自己的 FTP 服务器，图 2-54 是 IIS 中【默认 FTP 站点属性】配置界面。



图 2-54　【默认 FTP 站点属性】配置界面

【问题 1】(2 分)

通常，FTP 服务器默认的【TCP 端口】是__(1)__，本题中 FTP 服务器采用主动模式传输数据，若按照图 2-54“TCP 端口”配置为 600，则其数据端口为__(2)__。

(1)　A．21　　B．23　　C．25　　D．80

(2)　A．600　　B．599　　C．21　　D．601

【问题 2】(3 分)

该单位在建立 FTP 服务器时，根据需求制定了如下策略：FTP 站点允许匿名登录，匿

名用户只允许对 FTP 的根目录进行读取操作；user1 可以对 FTP 根目录下的 aaa 目录进行完全操作，user2 用户可以对 FTP 根目录下的 bbb 目录进行完全操作。

根据策略要求，网络管理员创建了 user1、user2 两个用户，并对 FTP 的根目录和 aaa 及 bbb 目录进行了用户权限配置。请参照图 2-55，按照策略说明给出下列权限：

Administrators 组对 FTP 根目录有__(3)__权限。

Everyone 组对 FTP 根目录有__(4)__权限。

user1 用户对 aaa 目录有__(5)__权限。

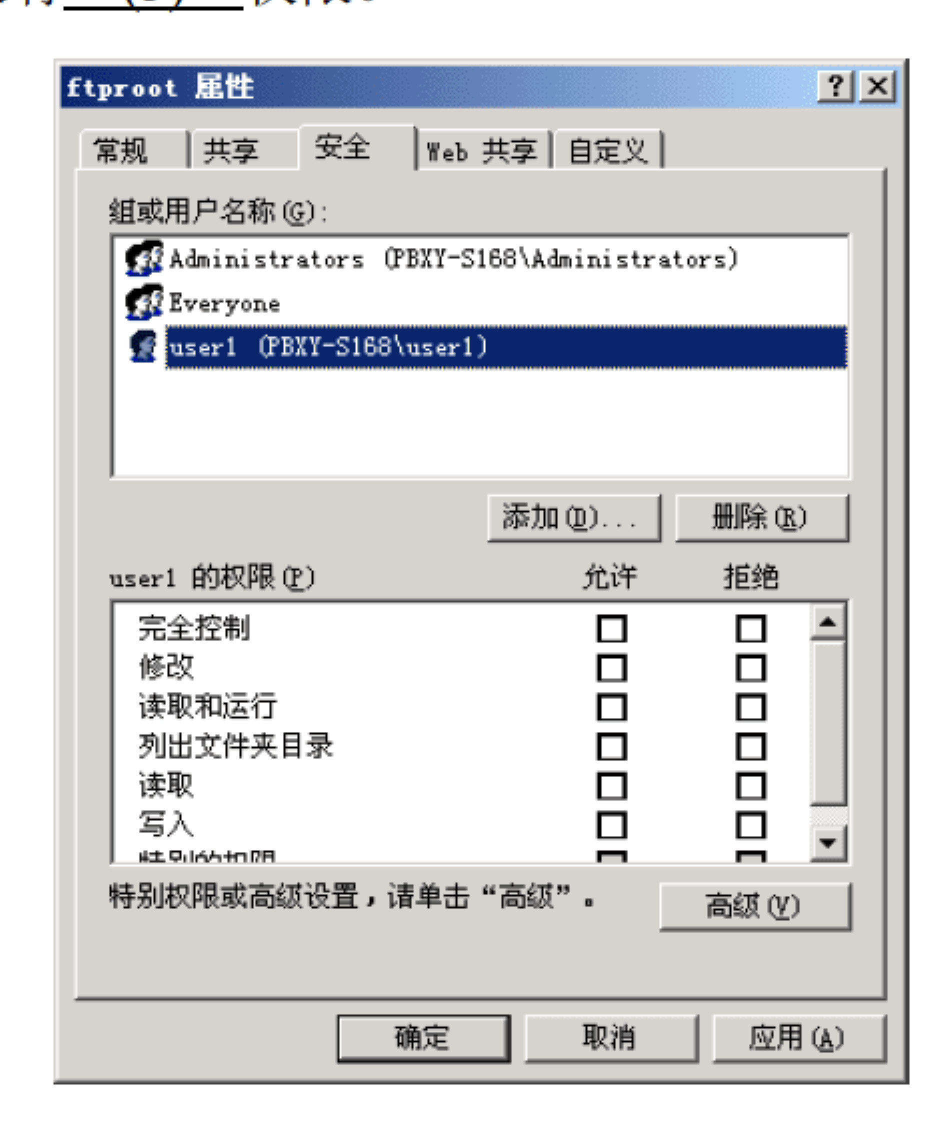


图 2-55　用户权限配置界面

【问题 3】(6 分)

请完成以下命令。

```
ftp>__(6)__            //连接 ftp.test.com 服务器
ftp>__(7)__            //把远程文件 test.txt 下载到本地
ftp>__(8)__            //将用户密码由 abc 改为 123
```

【问题 4】(3 分)

图 2-56 为该 FTP 服务器的安全帐号配置，FTP 客户端进行匿名登录时，默认的用户名是__(9)__。

A．IUSR_NETCENTE-KHD4U　　　　B．Everyone

C．Anonymous　　　　D．Admvinisvtratvors

分析：

【问题 1】

FTP 使用两条 TCP 连接来完成文件传输，一条用于传送控制信息(命令和响应)，另一条用于数据发送。在默认情况下，在服务器一端的控制连接使用的端口号是 21，数据连接使用的端口号为 20。

FTP 协议有主动连接(PORT)和被动连接(PASV)两种方式。当使用主动连接(PORT)时，FTP 默认端口修改后，数据连接端口也发生了改变。例如，若 FTP 的 TCP 端口配置为 600，

则其数据端口为 599。

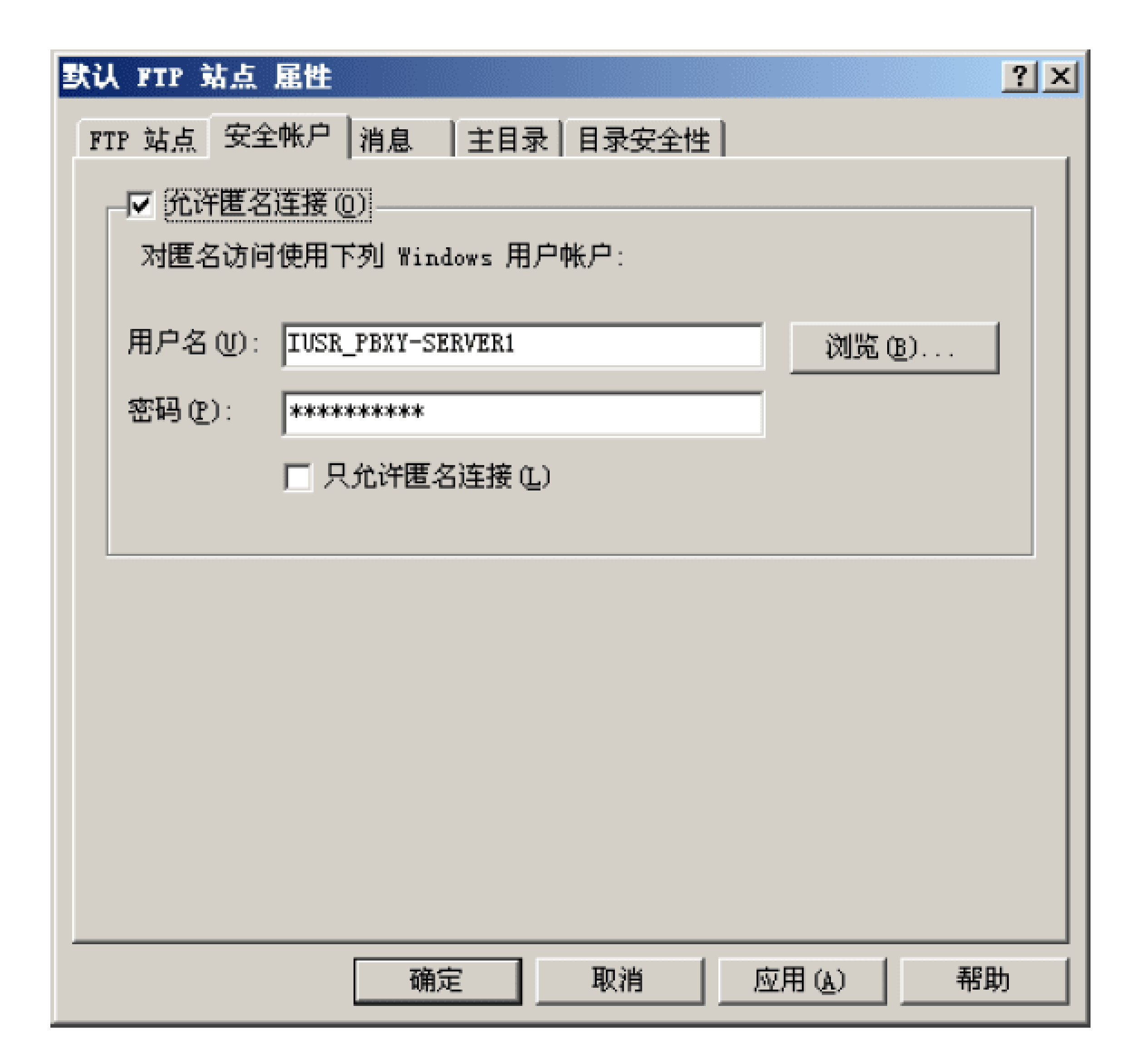


图 2-56　【安全帐户】配置界面

【问题 2】

为了方便管理，系统管理员组(Administrators)的用户应当对 FTP 根目录有“完全控制”权限；由于 FTP 站点允许匿名登录，并且只允许匿名用户对 FTP 的根目录进行读取操作，因此 FTP 根目录有“读取”权限。要实现 user1 可以对 FTP 根目录下的 aaa 目录进行完全操作，就要使用 user1 用户对 aaa 目录有“完全控制”权限。

【问题 3】

对于空(1)，连接 FTP 服务器的命令是 open，语法是：

```
open <服务器 IP 地址或域名> [端口号]
```

对于空(2)，从 FTP 服务器中下载文件的命令有 3 个：get 或 recv 的功能是从服务器中下载一个文件到本地计算机上，而 mget 的功能是下载多个文件，并支持通配符。

对于空(3)，修改用户密码的命令是 quote site pswd，语法是：

```
quote site pswd <旧密码> <新密码>
```

【问题 4】

Windows 操作系统在安装 IIS 组件后，将自动创建一个“IUSR_计算机名”的用户帐号，该帐号是 Web 服务器和 FTP 服务器匿名访问帐号。但是 FTP 服务器的通用匿名帐号是 Anonymous。上述帐号是不统一的，因此 FTP 客户端要匿名登录时，FTP 会把 Anonymous 映射成“IUSR_计算机名”，以方便用户使用。

答案：

【问题 1】

(1)　A

(2)　B

【问题 2】

(3) 完全控制(或 Full control)

(4) 读取(或 Read)

(5) 完全控制(或 Full control)

【问题 3】

(6) open ftp.test.com

(7) get test.txt

(8) quote site pswd abc 123

【问题 4】

(9) C

2.4.3 同步练习

1．阅读以下说明，回答问题 1～问题 4，将答案填入对应的答案栏内。

【说明】

某公司使用一台装有 Windows Server 2003 的 PC 服务器作为 Web 服务器(文档的主目录为 D:\www/root)。为了使 Web 管理员(其用户名为 webadmin)能够上传主页，系统管理员在这台服务器上安装了 IIS 并配置了 FTP 服务。为了信息安全，必须对这台服务器的 FTP 作一些控制。下面是一些要求，请回答如何设置。

【问题 1】不使用 FTP 默认 TCP 端口 21 作为服务器端口，而改用 TCP 端口 8089。

【问题 2】禁止匿名用户访问该台服务器上的 FTP 服务。

【问题 3】只能在 IP 地址为 210.45.12.31 的主机上上传或下载主页数据。

【问题 4】如果想要用户 webadmin 使用 FTP 登录时，直接进入 Web 服务器的文档主目录。

2．阅读以下说明，回答问题 1～问题 4，将答案填入对应的答案栏内。

【说明】

某公司使用一台装有 Windows Server 2003 的 PC 服务器作为 FTP 服务器，主要用于内部文件下载。该公司的网络地址是 192.168.10.0/24 这个 C 类地址，内部文件都存放在“D:\公用文件”下，另外每个用户都在该服务器上有一个帐号和自己的主文件夹(主文件夹都不在“D:\公用文件”下)。

【问题 1】若该公司内部所有的用户使用匿名用户就可以下载内部文件，FTP 站点主目录设置成什么？如何设置？

【问题 2】为保证外网的用户不能访问该 FTP 站点，如何设置？

【问题 3】由于该服务器还提供其他服务，必须限制最大在线人数为 100，如何实现这一功能？

【问题 4】如果想让每个用户使用自己的帐号登录该服务器时，就直接进入自己的主文件夹，如何实现这一功能？

2.4.4　同步练习参考答案

1.

【问题 1】打开 FTP 站点属性窗口，在【FTP 站点】选项卡的【TCP 端口】文本框中将 21 改为 8089，再重新启动 FTP 服务。

【问题 2】在【安全帐户】选项卡中，取消选中【允许匿名连接】复选框，即可禁止用户匿名访问该 FTP 站点。

【问题 3】在【目录安全性】选项卡中，选中【拒绝访问】单选按钮，单击【添加】按钮，在弹出的对话框中，选中【单机】单选按钮，再在【IP 地址】文本框中输入 210.45.12.31。

【问题 4】新建一个别名为 webadmin 的虚拟目录，其实际位置为 D:\wwwroot，并将访问权限设置为【读取】和【写入】。

2.

【问题 1】主目录应设置为“D:\公用文件”。操作步骤是：在 FTP 站点的属性窗口中，切换到【主目录】选项卡，选中【此计算机上的目录】单选按钮；在【FTP 站点目录】选项区域中，单击【浏览】按钮，选择“D:\公用文件”，或者直接输入“D:\公用文件”。

【问题 2】设置目录安全性的具体操作步骤是：在 FTP 站点的属性窗口中，切换到【目录安全性】选项卡，选中【拒绝访问】单选按钮，单击【添加】按钮；在【授权以下访问】对话框中，选中【一组计算机】单选按钮，在【网络标识】文本框中输入 192.168.10.0，在【子网掩码】文本框中输入 255.255.255.0。

【问题 3】设置最大连接数。具体操作步骤是：在 FTP 站点的属性窗口中，切换到【FTP 站点】选项卡，选中【连接限制为】单选按钮，并在后面填入 100。

【问题 4】在 FTP 站点中，为每一个用户建立和用户名相同的虚拟目录，其真实路径指向该用户的主文件夹，并将权限设置为【读取】和【写入】。

2.5　Web 服务器配置

2.5.1　考点辅导

2.5.1.1　Windows 2003 IIS 中 Web 服务器的配置

(1)　Web 站点的基本配置如图 2-57 所示。

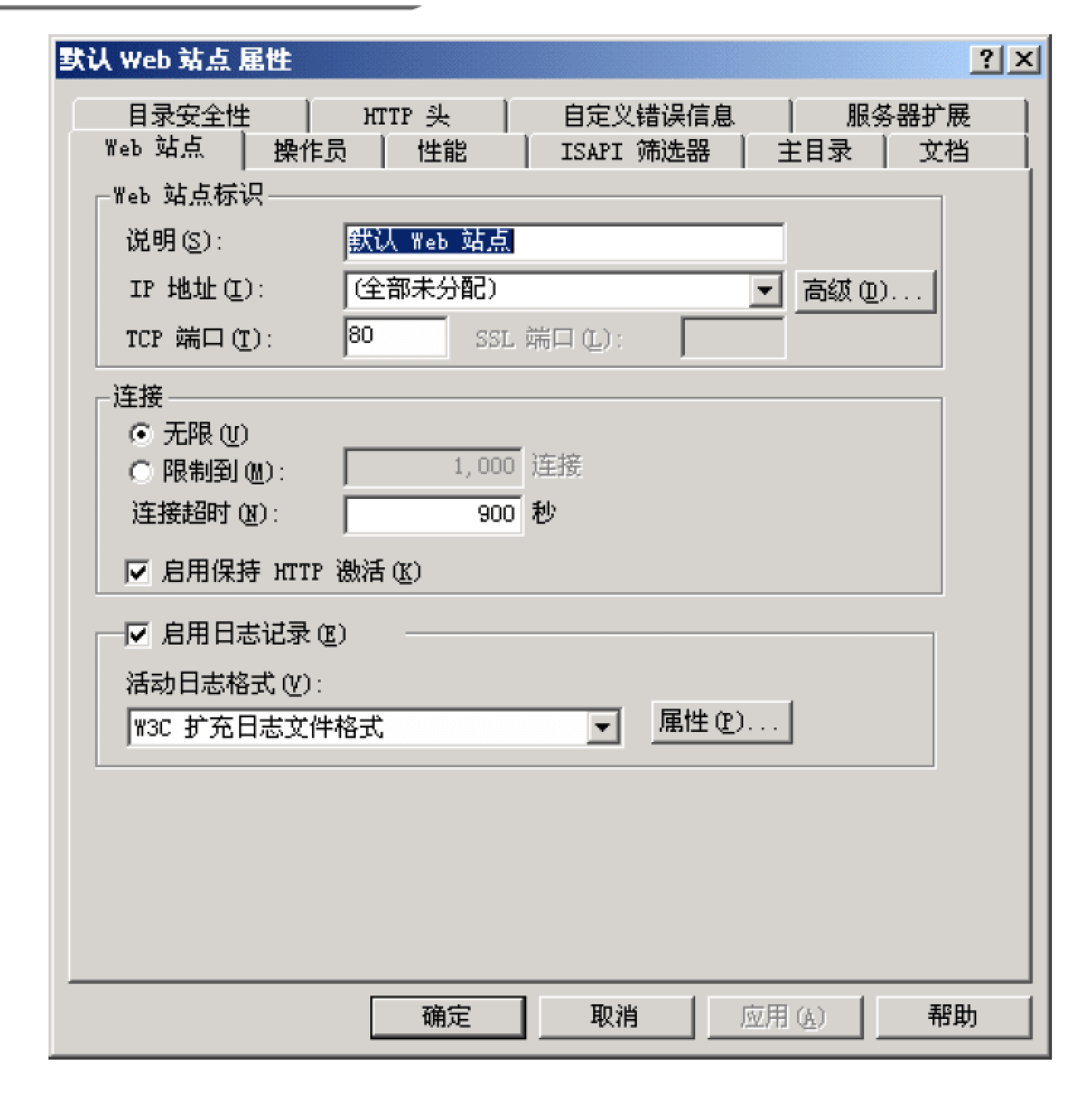


图 2-57 【Web 站点】选项卡

Web 站点的基本信息配置及其含义如表 2-7 所示。

表 2-7 Web 站点的基本配置

配置内容	配置项	说　明
Web 站点标识	说明	显示在 IIS 控制台的名称，以示区别各个站点
	IP 地址	Web 服务器对外服务的 IP 地址
	TCP 端口	Web 服务器服务的 TCP 端口号，默认为 80。若不是 80，则访问时必须在 URL 中指出
	SSL 端口	使用安装套接字访问(用 https://)的端口号，默认为 443
	【高级】按钮	除修改 IP 地址、端口号外，还可修改站点的主机头
连接	无限	对同时连接站点的用户数量不作限制
	限制到	根据实际情况限制同时连接站点的用户数量
	连接超时	如果用户在规定的时间内没有与 Web 服务器进行信息交换，则自动中断此用户的连接
	启用保持 HTTP 激活	允许客户端保持与服务器的开放连接
日志	启用日志记录	日志是用来记录服务器的访问、错误等信息，需要设置日志格式、日志记录内容、记录方法等

(2) 目录安全性设置如图 2-58 所示。

① 匿名访问和验证控制。单击【编辑】按钮，弹出【验证方法】对话框。其中，有 4

种验证方式，具体如下。

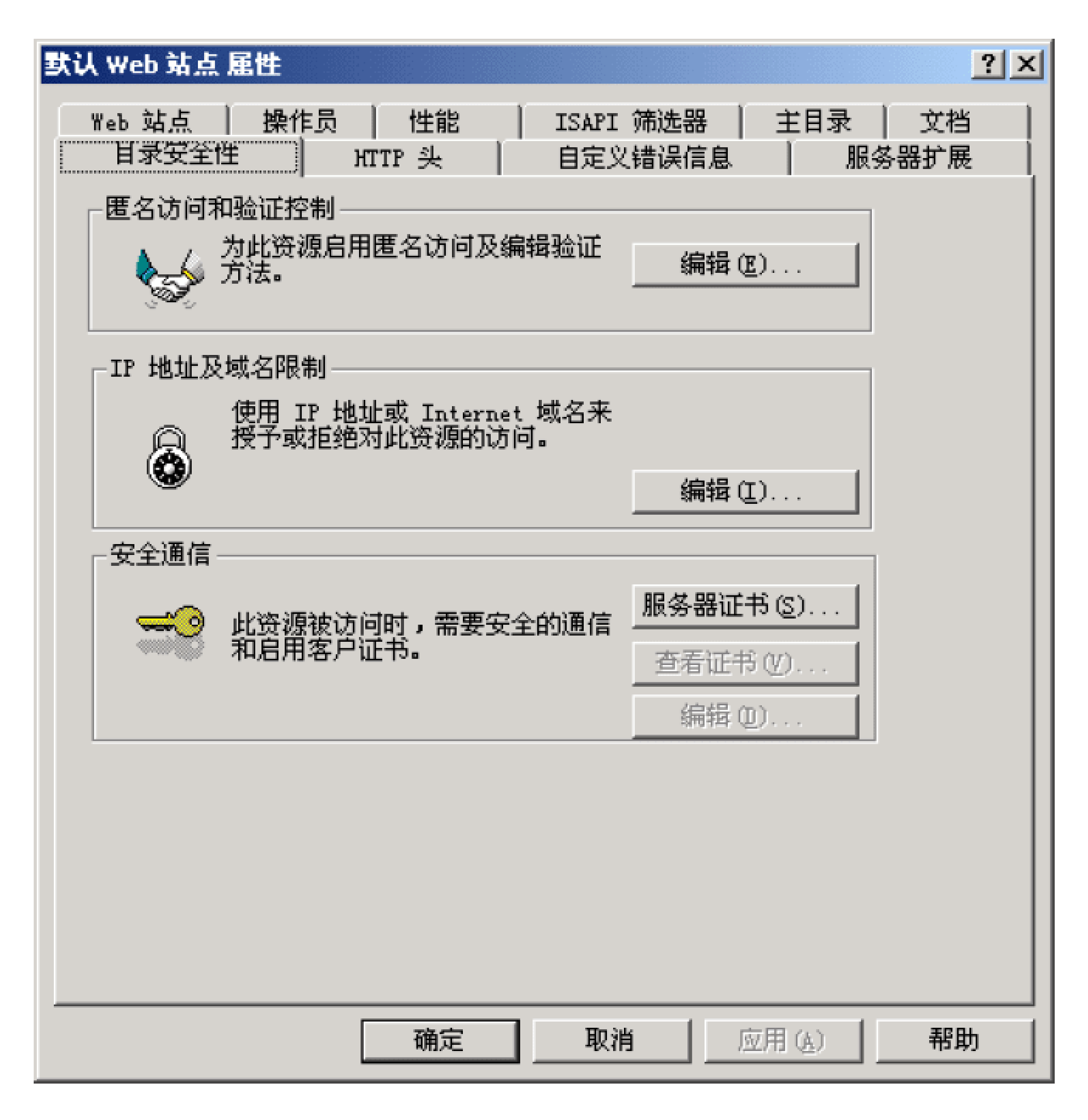


图 2-58 【目录安全性】选项卡

- 匿名访问：任何用户都可以连接网站，不需要输入用户帐号和密码。目前所有的浏览器都支持这种方式。在安装 IIS 时，系统自动创建一个用来代表匿名的帐号，该帐号的名称为“IUSR_计算机名”。
- 基本验证：要求用户输入帐号和密码，但密码都是以明文形式发送的。
- Windows 域服务器的摘要验证：只能在 Windows 2000 的域环境下用。
- 集成 Windows 验证：也要求用户输入帐号和密码，但密码在网络中传送之前，经过了散列处理，从而保证了密码的安全。有两种验证方法：Kerberos V5 验证和 NTLM。

② IP 地址及域名限制。单击【编辑】按钮，弹出【IP 地址及域名限制】对话框。其中，有两种方式来限制 IP 地址的访问，具体如下。

- 授权访问：其含义是除列表中 IP 地址的主机不能访问外，其他所有主机都可以访问该站点。主要用于给 Web 服务器加入“黑名单”。
- 拒绝访问：其含义是除列表中 IP 地址的主机能访问外，其他所有主机都不能访问该站点。主要用于内部 Web 站点，以防止外部主机访问该 Web 站点。

③ 安全通信。要保证客户端和站点进行安全的通信，需结合“证书服务”。

(3) 主目录的配置如图 2-59 所示。

主目录的配置的基本含义如表 2-8 所示。

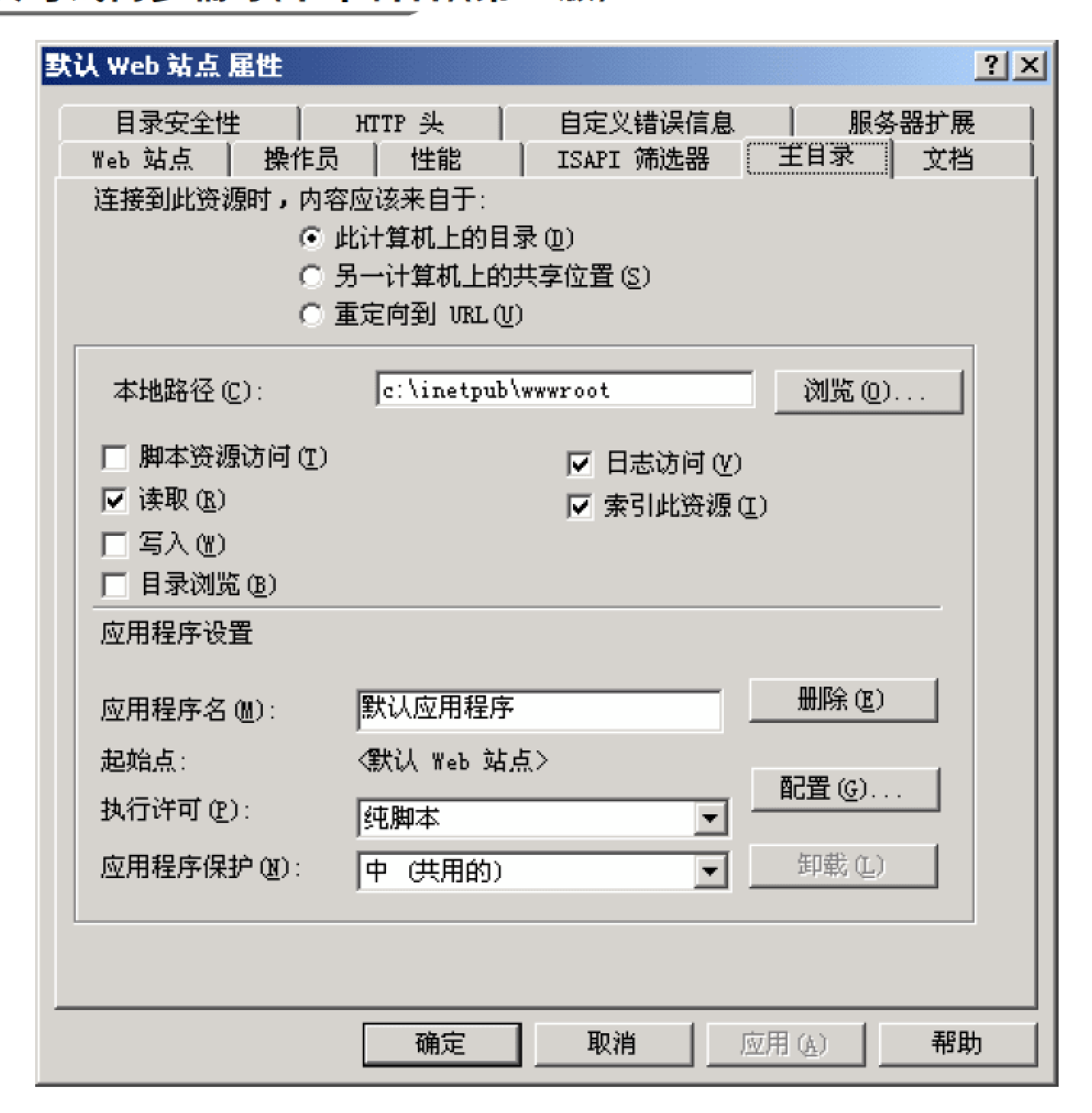


图 2-59 【主目录】选项卡

表 2-8 主目录的配置

配置内容	配置项	说 明
权限设置	脚本资源访问	是否允许用户访问程序中的脚本资源
	读取	是否允许用户读取站点内容及相关属性
	写入	是否允许用户上传文件到已启用的目录
	目录浏览	当目录中没有默认文档时，是否允许用户浏览目录中的文本列表
	日志访问	是否在日志文件中记录对目录的访问
	索引此资源	是否允许 Microsoft Indexing Service 将该目录包含在 Web 站点的全文索引中
应用程序设置	执行许可	无：只允许访问 HTML、图像文件等静态文件 纯脚本：允许运行 ASP 等编程脚本 脚本和可执行程序：除脚本之外，还可以执行应用程序
	应用程序保护	较低：应用程序与 Web 在同一进程中运行 中等：与其他应用程序一起在一个独立的共用进程中运行 较高：应用程序在一个独立的进程中运行

注：从安全性考虑，只需赋予用户【读取】的权限即可，而不要赋予其他的权限。

(4) 默认文件的配置如图 2-60 所示。

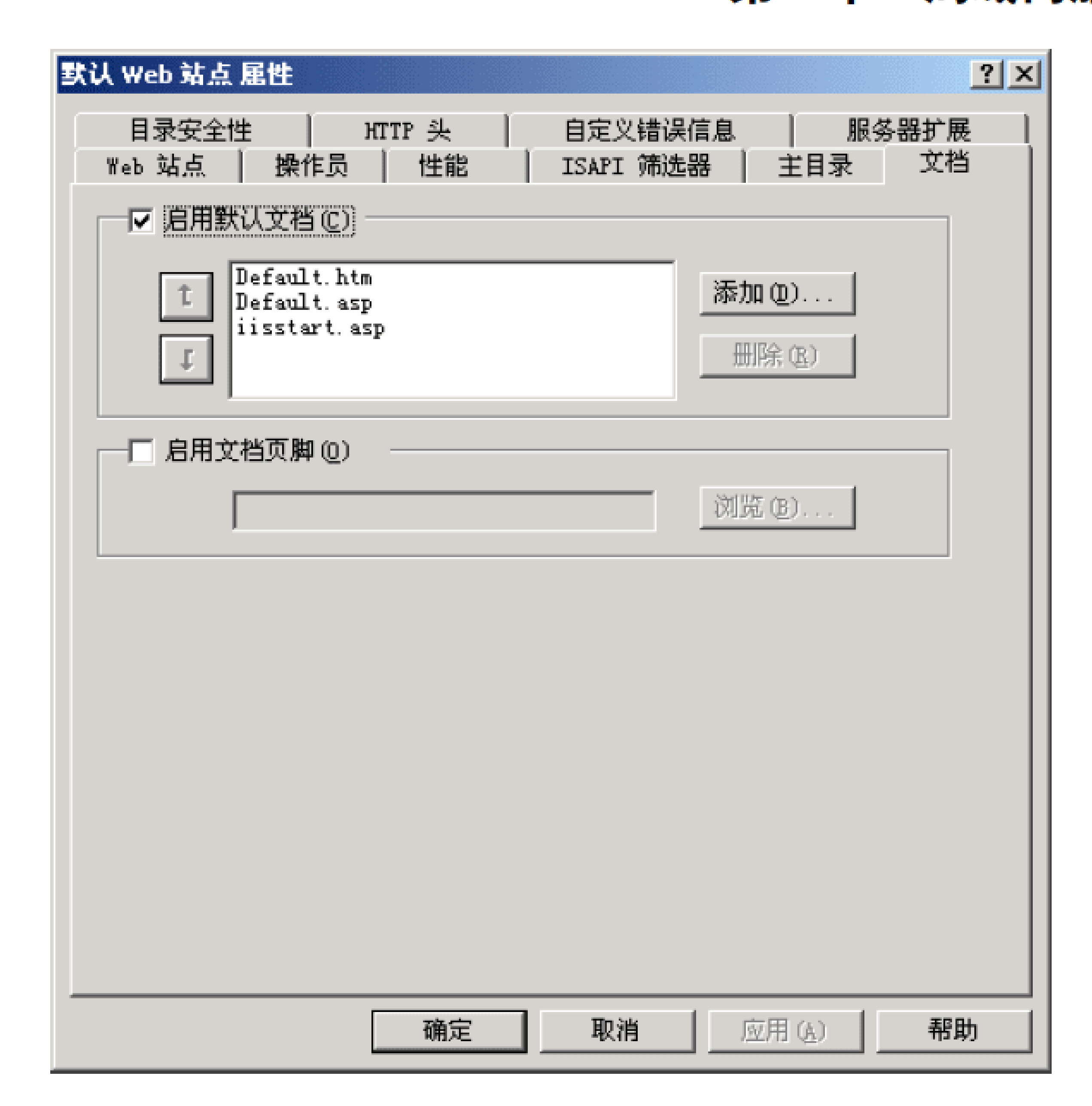


图 2-60 【文档】选项卡

- 启用默认文档：图中系统设置了 3 个网页，它会先读取最上面的文件(Default.htm)，若在主目录中没有该文件，则依次读取后面的文件。可以通过“↑”、“↓”两个按钮来调整系统读取这些文件的顺序，也可以通过【添加】和【删除】按钮增加或删除默认网页。
- 启用文档页脚：如果希望让网站中的每一个网页的最后都插入公司名称、商标图形、版权说明等信息，可以选中【启用文档页脚】复选框，然后在文本框中输入该文档脚本的路径和文件名。

(5) 虚拟主机的设置。

① 设定虚拟主机方式：

- 基于 IP 方式(IP-Based)：在服务器上设置多个 IP 地址，每个 IP 地址对应一台虚拟主机，访问时可以使用 IP 地址，也可以使用域名。
- 基于域名方式(Name- Based)：在 HTTP 1.1 标准中规定了对浏览器和服务器通信时，服务器能够跟踪浏览器请求的是哪个主机名字。服务器只需要一个 IP 地址，但对应着多个域名，每个域名对应一台虚拟主机，是建立虚拟主机的标准方式。访问时，只能使用域名访问。
- 基于 TCP 连接端口：每个虚拟主机分别拥有一个惟一的 TCP 端口号，访问时需要加上 TCP 端口号。

② 配置方法：在【Web 站点创建向导】的【IP 地址和 TCP 端口设置】对话框中(如图 2-61 所示)，根据上述三种虚拟主机的实现方式，分别作不同的设置。

- 基于 IP 方式的虚拟主机：在【输入 Web 站点使用的 IP 地址】下拉列表中选择合适的 IP 地址。
- 基于域名方式的虚拟主机：在【此站点的主机头】的文本框中输入虚拟主机的域名。



图 2-61　创建虚拟主机

- 基于 TCP 端口的虚拟主机：在【此 Web 站点应使用到的 TCP 端口】文本框中输入主机的 TCP 端口号。

(6) 虚拟目录：将一个 URL 以非标准方式映射到一个目录文件名，也就是说可以将文档存储在服务器定义的主目录以外的位置。

2.5.1.2　Red Flag Linux 下 Apache Web 服务器的配置

1. *启动 rfapache*

rfapache 配置工具需要在 KDE 环境下以 root 权限运行。非 root 用户虽然允许运行和使用配置工具，但由于没有权限修改配置文件，所以即使在配置工具中修改了选项也无法保存和生效。启动 rfapache 配置工具有以下三种方式。

(1) 在系统菜单中选择【系统】|【控制面板】命令，打开【控制面板】窗口，在【网络服务配置】选项卡中，双击【Apache 配置工具】。

(2) 在系统主菜单中选择【管理工具】|【Apache 配置工具】命令。

(3) 在运行命令行或 shell 提示符下直接输入 rfapache。

rfapache 的配置主界面窗口左侧是 Apache Server 的控制台树，显示了服务器主机中已建的主机站点和目录的树状结构；窗口右侧从上到下依次为列表显示区、配置文件编辑器、配置文件跳转器和消息显示窗口。在左侧的控制台树中选中某一节点时，列表显示区中将出现该节点中的内容，可以按名称、类型或路径名排序。如果选中的是一个目录，则显示该目录中的所有子目录和文件。管理员可以在配置文件编辑器中手工修改配置文件，并保存。消息显示窗口显示的是 Apache 服务器启动、重启、停止或校验配置文件等的输出信息。

2. *启动、停止和重新启动 Apache 服务*

打开 Apache 配置工具 rfapache，可在主界面窗口中进行以下操作。

- 选择【操作】|【启动】命令，启动 httpd 服务。
- 选择【操作】|【停止】命令，停止 httpd 服务。

- 选择【操作】|【重启】命令，重新启动 httpd 服务。

如果 httpd 服务已经启动，那么菜单项【操作】|【启动】不可用；如果 httpd 服务没有启动，那么菜单项【操作】|【停止】和【操作】|【重启】不可用。操作结果的输出信息将显示在消息窗口中。

管理员也可以在命令行终端下启动、停止和重新启动 Apache，命令分别是：

```
#/etc/init.d/httpd start
#/etc/init.d/httpd stop
#/etc/init.d/httpd restart
```

3. 添加和删除虚拟主机

虚拟主机是指在一个单一的服务器上维护多个 Web 站点，并且使用主机别名来区别它们。这样用户就可以在单一的 Web 服务器上拥有多个 Web 站点，并通过它们各自的域名对这些站点进行访问，而无须了解任何其他路径信息。

随着 Internet 上的 Web 站点数目的逐渐增多，在一台服务器上有效托管多个 Web 站点的能力已经成为第一流 Web 服务器引擎的关键特性。Apache 提供了对虚拟主机的完全支持。虚拟主机一般有两种形式：“基于名字”和“基于 IP”。

1) 添加虚拟主机

Apache 配置工具中提供了一个虚拟主机的创建向导。打开 rfapache，选择【操作】|【添加虚拟主机】命令，或者单击工具栏中的【添加虚拟主机】按钮，按照【虚拟主机创建向导】中的提示完成操作。

通过这个向导，管理员可以定义虚拟主机的主机名、IP 地址和端口、主目录以及规划用户的访问权限等；在向导的最后，还列出了新建虚拟主机的概要信息。创建虚拟主机时，需要保证所创建的虚拟服务器名称能够在 DNS 中正确解析。

当设置出现下列问题的时候，工具将给出错误提示，提示重新设置。

- 对于“基于名称”的虚拟主机，设置的主机名已经被其他虚拟主机使用。
- 对于“基于 IP”的虚拟主机，选择的 IP 地址(端口)已经被其他虚拟主机使用。
- 指定的主目录不存在或不是一个合法的路径。

2) 删除虚拟主机

在 rfapache 配置工具主窗口左侧的控制台树中，选择需要删除的虚拟主机名。然后选择菜单中的【操作】|【删除】命令，或单击工具栏中的【删除】按钮，当被询问是否确认要删除该主机时，单击【确定】按钮即可。

4. 添加和删除虚拟目录

虚拟目录的概念源于 Alias 和 ScriptAlias 指令，一般称为“别名”。这样的指令可以将一个 URL 以非标准方式映射到一个目录文件名，也就是说，可以将文档存储在服务器定义的主目录以外的位置。通过别名访问时，要在别名后加一个斜线后缀“/”。

1) 创建虚拟目录

在 rfapache 配置工具主窗口左侧的控制台树中，选择虚拟目录要添加的位置(默认主机或者是虚拟主机)。然后选择菜单中的【操作】|【添加虚拟目录】命令，或者单击工具栏中的【添加虚拟目录】按钮，在弹出的【虚拟目录创建向导】对话框中，根据提示创建一个

新的虚拟目录。利用这个向导，管理员可以定义虚拟目录的别名、目录的路径及规划用户的访问权限等；在向导的最后，列出了新建虚拟目录的概要信息。

当设置出现下列问题的时候，工具将给出错误提示，提示重新设置。

- 设置的别名已经存在。
- 设置的目录路径不合法。
- 设置的目录已经被其他别名映射。

2) 删除虚拟目录

在 rfapache 配置工具主窗口左侧的控制台树中，选择需要删除的虚拟目录。然后选择菜单中的【操作】|【删除】命令，或单击工具栏中的【删除】按钮，当被询问是否确认要删除该虚拟目录时，单击【确定】按钮即可。

5. 设置属性

可以在配置工具 rfapache 中设置“默认主机”、“虚拟主机”和“虚拟目录”的属性。

在 rfapache 配置工具主窗口左侧的控制台树中，选择需要查看或设置属性的主机或目录，选择菜单中的【操作】|【设置属性】命令，或者单击工具栏中的【设置属性】按钮，也可以右击，从弹出的快捷菜单中选择【设置属性】命令，在弹出的属性设置窗口中查看或修改相应的属性。属性设置窗口中包括多个配置选项卡，具有相当多的选项可供设置，分别说明如下。

(1) 站点属性：使用此选项卡设置站点的标识参数和日志信息等。只有默认主机和虚拟主机有此选项卡。主要包括：①站点属性：站点名称(配置项：ServerName)、管理员 E-mail(配置项：ServerAdmin)、IP 地址和 TCP 端口；②错误日志：日志位置(配置项：ErrorLog)、日志级别(配置项：LogLevel)；③自定义日志：日志位置(配置项：Customlog)、日志格式、详细格式(配置项：LogFormat)。

(2) 主目录：使用此选项卡修改主目录的路径(配置项：DocumentRoot)、设置主目录的执行属性(配置项：Options)和目录别名(配置项：Alias)。

(3) 访问许可：用来根据 IP 地址或域名等来授权或者禁止对资源的访问。主要包括：访问顺序(配置项：Order)，基本上有两种形式，即先禁止后允许和先允许后禁止；允许访问列表(配置项：Allow from)；禁止访问列表(配置项：Deny from)。

(4) 默认文档：使用此选项卡定义站点的默认页面。默认文档的配置项是 DirectoryIndex。在这里设置请求指定目录时该目录的索引文件，用户可以定义多个这样的索引文件。若要添加新的默认文档，单击【添加】按钮即可。

(5) 错误信息：其配置项是 ErrorDocument。如果 Apache 在处理用户请求时遇到错误，它将按照配置显示一个标准错误页；给出 HTTP 响应代码；使用 ErrorDocument 指令并针对标准 HTTP 错误来自定义成用户的错误响应，以便用户更容易理解。针对虚拟主机设置的错误信息会继承默认主机中的值；同样，虚拟目录的默认文档也会继承虚拟主机(或默认主机)中的值。如果要添加新的自定义错误消息，可单击【添加】按钮；如果要更改某一错误消息的属性，单击【编辑】按钮；如果要删除某一自定义错误消息，单击【删除】按钮。

(6) 性能：用来设置一些和 Apache 运行性能有关的配置项。只有“默认主机”包含此选项卡。主要包括：保持连接(配置项：KeepAlive)、保持连接时间(配置项：KeepAliveTimeout)、

最大请求保持数(配置项：MaxKeepAliveRequests)、连接超时(配置项：TimeOut)、初始化最大进程数(配置项：StartServers)、最小空闲进程数(配置项：MinSpareServers)、最大空闲进程数(配置项：MaxSpareServers)、单进程最大请求数(配置项：MaxRequestsPerchild)、最大连接数(配置项：MaxClients)。

(7) 杂项：用来设置一些其他的常用且很重要的配置项。只有“默认主机”包含此选项卡。主要包括：服务器根目录(配置项：ServerRoot)、服务 PID 文件(配置项：PidFile)、服务 LOCK 文件(配置项：LockFile)、用户名(配置项：User)、组名(配置项：Group)。

2.5.1.3　Linux 下 Apache Web 服务器的安装与配置

1. Apache Web 服务器的安装

如果用户在安装 Linux 时一并安装了 Apache Web 服务器，就不需再另行安装。如果用户不能确定是否已经安装了 Apache Web 服务器，可以通过执行以下命令检查：

```
#rpm -qa |grep apache
apache-1.3.20-16            //若出现此行，则表示已经安装了 Apache 主程序
apache-0.8.1-1              //若出现此行，则表示已经安装了 Apache 配置文件
apache-devel-1.3.20-16      //若出现此行，则表示已经安装了 Apache 开发工具软件
apache-manual-1.3.20-16     //若出现此行，则表示已经安装了 Apache 说明文件
```

如果用户发现系统未安装 Apache Web 服务器，可以从网上下载 Apache Web 服务器的安装包，也可以在 Red Hat Linux 安装盘中找到 Apache Web 服务器安装包。其安装命令是：

```
#rpm -ivh apache*.rpm           //安装 Apache Web 服务器
```

如果用户想从旧版本的 Apache Web 服务器升级到新的版本，只需把执行参数“-i”改为“-U”即可，其命令如下：

```
#rpm -Uvh apache*.rpm           //更新 Apache Web 服务器
```

2. Apache Web 服务器的配置

如果安装时未指定安装目录，Apache 服务器的设置文件位于/usr/local/apache/conf/目录下，传统上使用三个配置文件——httpd.conf、access.conf 和 srm.conf 来配置 Apache 服务器的行为。

httpd.conf 提供了最基本的服务器配置，是对守护程序 httpd 的运行方式的技术描述；srm.conf 是服务器的资源映射文件，告诉服务器各种文件的 MIME 类型，以及如何支持这些文件；access.conf 用于配置服务器的访问权限，控制不同用户和计算机的访问限制。

事实上当前版本的 Apache 将原来 httpd.conf、srm.conf 与 access.conf 中的所有配置参数均放在了一个配置文件 httpd.conf 中，只是出于与以前版本兼容的原因(使用这三个设置文件的方式来源于 NCSA-httpd)，才使用三个配置文件。而提供的 access.conf 和 srm.conf 文件中没有具体的设置。

由于在新版本的 Apache 中，所有的设置都被放在了 httpd.conf 中，而 access.conf 和 srm.conf 文件中没有具体的设置。以下使用默认提供的 httpd.conf 为例，解释 Apache 服务器的各个设置选项。然而，不必因它提供的设置参数太多而烦恼，基本上这些参数都很明确，也可以不加改动即可运行 Apache 服务器。但如果需要调整 Apache 服务器的性能，以及增

加对某种特性的支持，就需要了解这些设置参数的含义。下面介绍几个常用的参数。

1) ServerType

ServerType 用来定义服务器的启动方式，默认值为独立方式 standalone。httpd 服务器将由其本身启动，并驻留在主机中监视连接请求。在 Linux 下将在启动文件/etc/rc.d/rc.local/init.d/apache 中自动启动 Web 服务器，这种方式是推荐设置。Apache 服务器工作在 standalone 方式时，代码为：

```
ServerType standalone
```

启动 Apache 服务器的另一种方式是 inetd 方式，使用超级服务器 inetd 监视连接请求并启动服务器。Apache 服务器工作在 inetd 方式时，代码为：

```
ServerType inetd
```

当需要使用 inetd 启动方式时，需要更改某些设置，从而屏蔽/etc/rc.d/rc.local/init.d /apache 文件。考虑到这种运行方式很少使用，这里就不作详细介绍了。

两种方式的区别是独立方式是由服务器自身管理自己的启动进程，这样在启动时能立即启动服务器的多个副本，每个副本都驻留在内存中，一有连接请求不需要生成子进程就可以立即进行处理，对于客户浏览器的请求反应更快、性能更高。而 inetd 方式要由 inetd 发现有连接请求后才去启动 httpd 服务器，由于 inetd 要监听太多的端口，因此反应较慢、效率较低，但节约了没有连接请求时 Web 服务器占用的资源。因此 inetd 方式只用于偶尔被访问并且不要求访问速度的服务器上。事实上，inetd 方式不适合 http 的突发和多连接的特性，因为一个页面可能包含多个图像，而每个图像都会引起一个连接请求，即使访问人数较少，但瞬间的连接请求并不少，这就受到 inetd 性能的限制，甚至会影响由 inetd 启动的其他服务器程序。

2) ServerRoot

ServerRoot 用于指定守护进程 httpd 的运行目录，httpd 在启动之后将自动将进程的当前目录改变为这个目录。因此，如果设置文件中指定的文件或目录是相对路径，那么真实路径就位于这个 ServerRoot 定义的路径之下。

3) Port

Port 定义了 Standalone 模式下 httpd 守护进程使用的端口，标准端口是 80。这个选项只对于以独立方式启动的服务器才有效，对于以 inetd 方式启动的服务器，则在 inetd.conf 中定义使用哪个端口。

4) ServerAdmin

ServerAdmin 用于配置 Web 服务器的管理员的 E-mail 地址，这将在 HTTP 服务出现错误的条件下返回给浏览器，以便让 Web 使用者和管理员联系，及时报告错误。习惯上使用服务器上的 webmaster 作为 Web 服务器的管理员，通过邮件服务器的别名机制，将发送到 webmaster 的电子邮件发送给真正的 Web 管理员。

5) ServerName

默认情况下，并不需要指定 ServerName 参数，服务器将自动通过名称解析过程来获得自己的名称；但如果服务器的名称解析有问题(通常为反向解析不正确)，或者没有正式的 DNS 名称，也可以在这里指定 IP 地址。当 ServerName 设置不正确的时候，服务器无法正

常启动。

6)　DocumentRoot

DocumentRoot 定义这个服务器对外发布的超文本文档所存放的路径，客户程序请求的 URL 就被映射为这个目录下的网页文件。这个目录下的子目录，以及使用符号连接指出的文件和目录都能被浏览器访问，只是要在 URL 上使用同样的相对目录名。

注意，符号连接虽然逻辑上位于根文档目录之下，但实际上可以位于计算机上的任意目录中，因此可以使客户程序能访问那些根文档目录之外的目录，这在增加了灵活性的同时却减少了安全性。Apache 在目录的访问控制中提供了 FollowSymLinks 选项来打开或关闭支持符号连接的特性。

7)　UserDir

当在一台 Linux 上运行 Apache 服务器时，这台计算机上的所有用户都可以有自己的网页路径，形如 http://example.abc.com.cn/～user，使用波浪符号加上用户名就可以映射到用户自己的网页目录上。映射目录为用户个人主目录下的一个子目录，其名称就用 UserDir 这个参数进行定义，默认为 public_html。如果不想为正式的用户提供网页服务，使用 DISABLED 作为 UserDir 的参数即可。

8)　DirectoryIndex

很多情况下，URL 中并没有指定文档的名称，而只是给出了一个目录名。那么 Apache 服务器就自动返回这个目录下由 DirectoryIndex 定义的文件，当然可以指定多个文件名称，系统会在这个目录下按顺序搜索。当所有由 DirectoryIndex 指定的文件都不存在时，Apache 服务器可以根据系统设置，生成这个目录下的所有文件列表，提供给用户选择。此时该目录的访问控制选项中的 Indexes 选项(Options Indexes)必须打开，以使得服务器能够生成目录列表，否则 Apache 将拒绝访问。

9)　Alias

Alias 参数用于将 URL 与服务器文件系统中的真实位置进行直接映射(虚拟目录)，一般的文档将在 DocumentRoot 中进行查询，然而使用 Alias 定义的路径将直接映射到相应目录下，而不再到 DocumentRoot 下面进行查询。因此，Alias 可以用来映射一些公用文件的路径，例如，保存了各种常用图标的 icons 路径。这样使得除了使用符号连接之外，文档根目录(DocumentRoot)外的目录也可以通过使用了 Alias 映射，提供给浏览器访问。定义好映射的路径之后，应使用 Directory 语句设置访问限制。

ScriptAlias 也是用于 URL 路径的映射，但与 Alias 的不同在于：ScriptAlias 用于映射 CGI 程序的路径，这个路径下的文件都被定义为 CGI 程序，通过执行它们来获得结果，而非由服务器直接返回其内容。默认情况下，CGI 程序使用 cgi-bin 目录作为虚拟路径。

10)　ErrorDocument

如果发生了某些意外情况，例如，用户请求的网页不存在，或者没有访问权限时，服务器将生成一个错误代码，同时也将回应用户浏览器一个标识错误的网页。

ErrorDocument 就用于设置当出现哪个错误时应该回应用户浏览器哪些内容。ErrorDocument 的第一个参数为错误的序号，第二个参数为回应的数据，可以是简单的文本、本地网页、本地 CGI 程序以及远程主机上的网页。例如：

```
ErrorDocument 404 /missing.html
```

```
ErrorDocument 404 /cgi-bin/missing_handler.pl
ErrorDocument 402 http://some.other_server.com/subscription_info.html
```

11) 虚拟主机

虚拟主机位于一台 Web 服务器上，可以为多个单独域名提供 Web 服务，并且每个域名都完全独立，包括具有完全独立的文档目录结构及设置。这样域名之间完全独立，不但使用每个域名访问到的内容完全独立，而且使用另一个域名无法访问其他域名提供的网页内容。

在 Apache Web 服务器中，有两种设定虚拟主机的方式：一种是 IP-Based(基于 IP 方式)，另一种是 Name-Based(基于域名方式)。下面是一个基于域名方式的配置示例：

```
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
   ServerAdmin webmaster@company1.com.cn
   DocumentRoot /www/htdocs/company1
   ServerName www.company1.com.cn
   ErrorLog logs/company1.com.cn -error_log
   CustomLog logs/ company1.com.cn-access_log common
</VirtualHost>
```

其中，NameVirtualHost 参数用来指定虚拟主机使用的 IP 地址(192.168.10.101)。这个 IP 地址将对应多个 DNS 名字。如果 Apache 使用了 Listen 参数控制了多个端口，那么就可以在这里加上端口号以进一步进行区分对不同端口的不同连接请求。<VirtualHost 192.168.10.101>……</VirtualHost>之间的语句用来设置虚拟主机相关参数，如管理员的邮箱(webmaster@company1.com.cn)、文档主目录(/www/htdocs/ company1)、服务器的域名(www.company1.com.cn)、错误日志(logs/company1.com.cn -error_log)和访问日志(logs/company1.com.cn-access_log common)的位置等。

3. *启动、停止和重新启动 Apache Web 服务器*

Apache Web 服务器守护程序为 httpd，当 Apache Web 服务器运行在 standalone(独立)模式下，可以通过 httpd 来启动、停止和重新启动 Apache Web 服务器。其命令分别是：#/etc/init.d/httpd start、#/etc/init.d/httpd stop、#/etc/init.d/httpd restart。

如果设定 Apache Web 服务器在计算机启动时自动启动或不启动，可以使用 ntsysv 命令将它加到引导程序中。也可以通过 chkconfig 命令来设定，该命令格式是：

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如我们希望计算机启动运行级别 3、5 时启动 Apache Web 服务器，则命令为：

```
#chkconfig --level 3 5 httpd on
```

再如，我们希望计算机启动运行级别 2 时不启动 Apache Web 服务器，则命令为：

```
#chkconfig --level 2 httpd off
```

如果希望在任何运行级别下启动时都不启动 Apache Web 服务器，只要不设定“[--level <运行级>]”就可以了，即

```
#chkconfig httpd on
#chkconfig httpd off
```

2.5.2　典型例题分析

例 1　阅读以下说明，回答问题 1～问题 5，将解答填入答案纸对应的解答栏内。(2008 年 5 月下午试题二)

【说明】

某公司欲建一小型网站对外发布产品信息，Web 服务器信息描述如下。

① 操作系统：Windows Server 2003，安装在 D 盘。

② 双网卡：IP 地址分别是 10.0.0.1 和 212.115.112.31。

③ 网站信息如表 2-9 所示。

表 2-9　某公司的网站信息表

名　称	灵便购机网
域名	www.mymobilephone.com
首页	mymobilephone.asp
网页存放位置	E:\web

用户可以在浏览器地址栏中输入 http://www.mymobilephone.com:8000 访问该网站。

【问题 1】(4 分)

填充如图 2-62 所示的【网站】选项卡。网站【IP 地址】文本框中应填入__(1)__，【TCP 端口】文本框中应填入__(2)__。

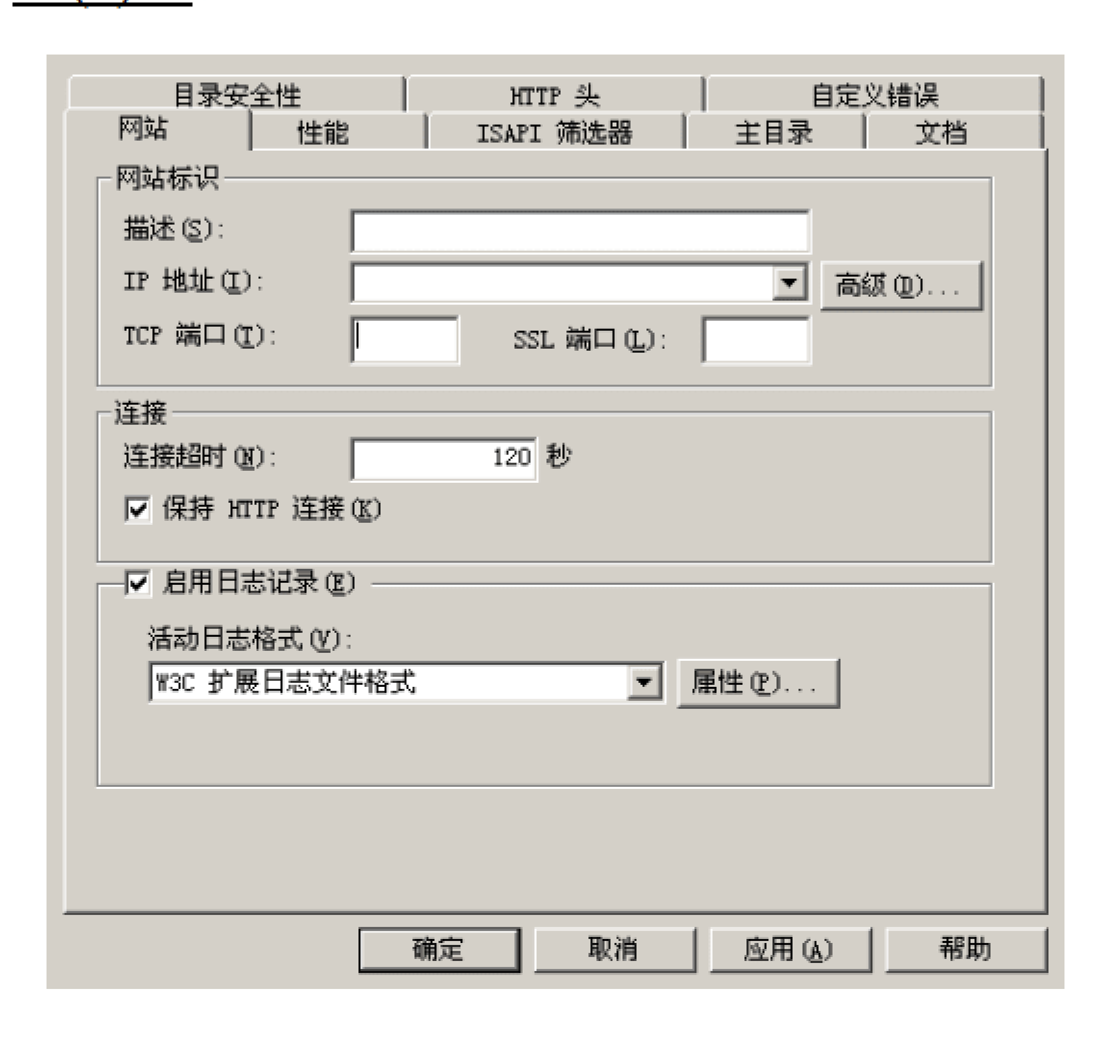


图 2-62　【网站】选项卡配置界面

【问题 2】(4 分)

填充如图 2-63 所示的【主目录】选项卡。【本地路径】文本框中默认情况下为__(3)__，现应填入__(4)__。

(3) A. E:\Internet　　B. D:\Internet\website

C. E:\Website　　D. D:\Inetpub\wwwroot

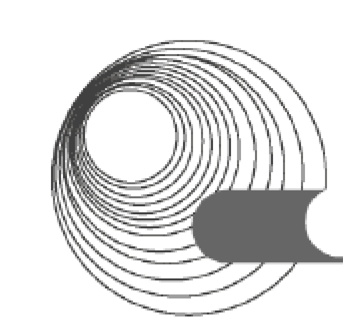




图 2-63 【主目录】选项卡配置界面

【问题 3】(3 分)

在 E:\web 目录中已有三个文件，如图 2-64 所示。为了使用户能正常访问该网站，在图 2-64 中应如何操作？

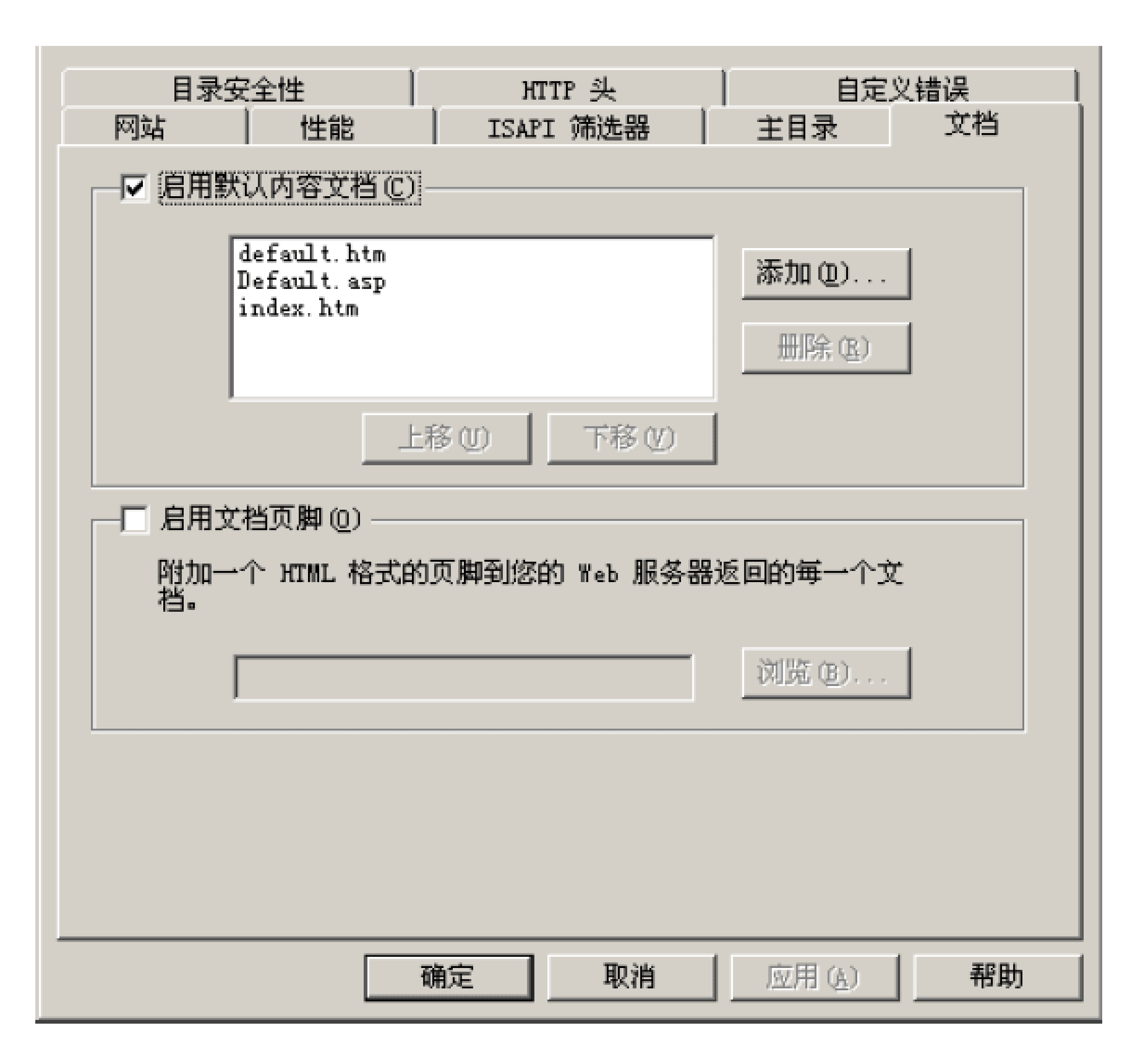


图 2-64 【文档】选项卡配置界面

【问题 4】(2 分)

为保障网站的安全性，需要单击图 2-65 中【IP 地址和域名限制】选项区内的【编辑】按钮，屏蔽某些恶意 IP 地址。如果要屏蔽 192.168.1.116，在图 2-66 中应如何操作？

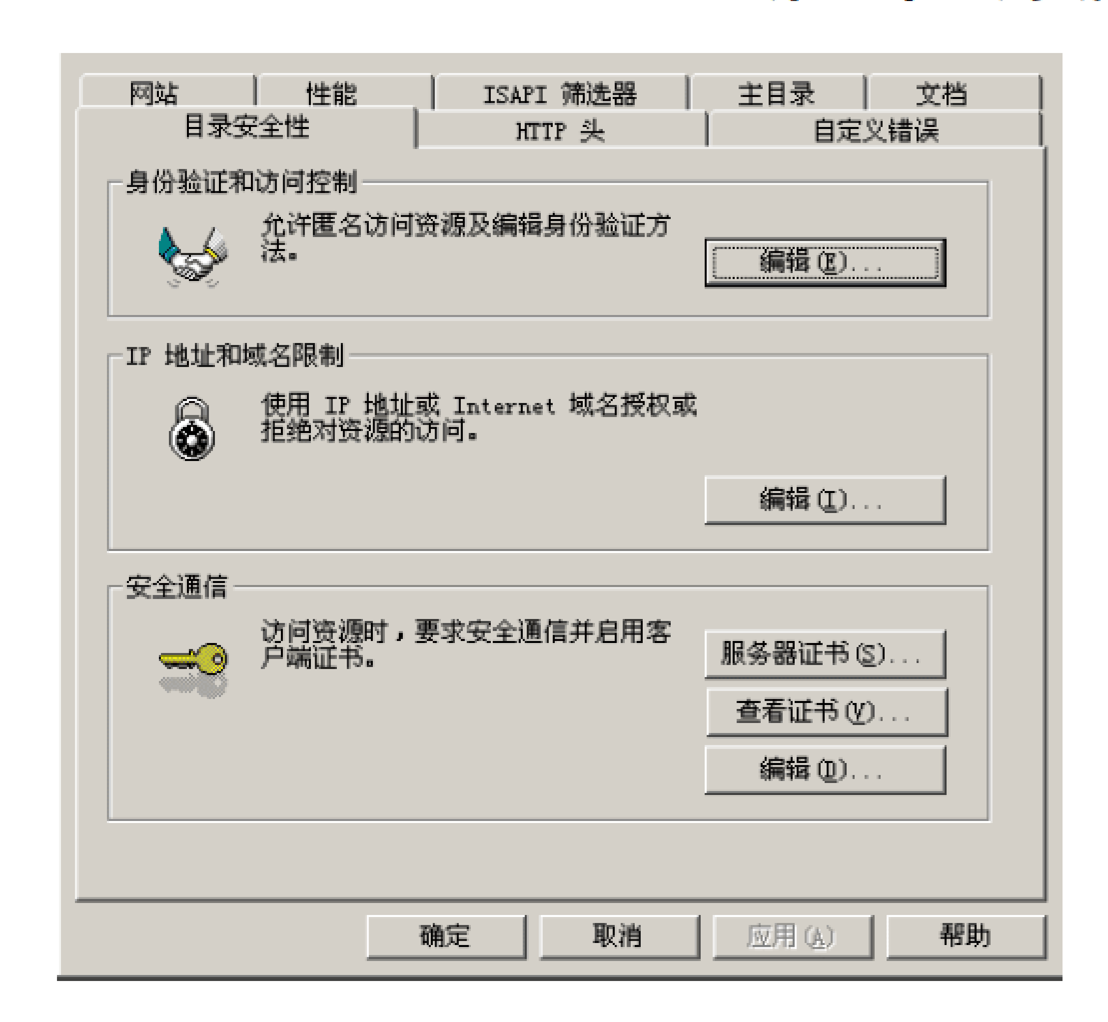


图 2-65　【目录安全性】选项卡

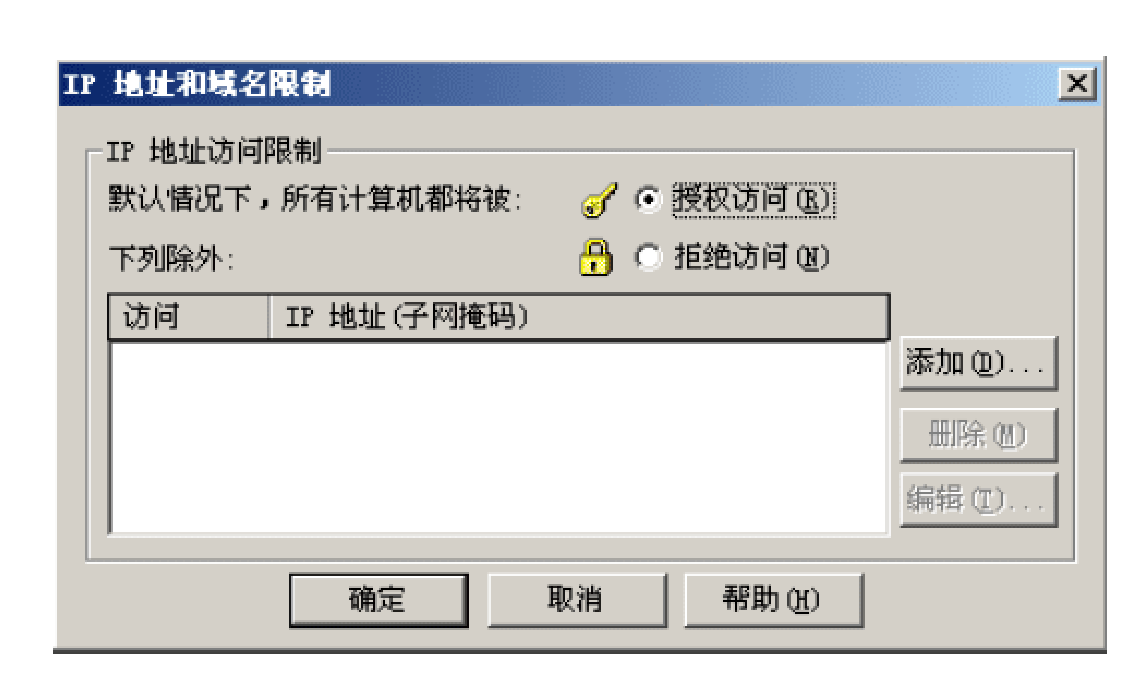


图 2-66　【IP 地址和域名限制】对话框

【问题 5】(2 分)

除了主目录以外，还可以采用__(5)__作为发布目录。

A. 备份目录　　B. 副目录　　C. 虚拟目录　　D. 活动目录

分析：

【问题 1】

本机为双网卡，分配了两个 IP 地址，分别是 10.0.0.1 和 212.115.112.31。10.0.0.1 为公司内网的 IP 地址，网站需要向外发布产品信息，因此要在【IP 地址】下拉列表框中选用公网 IP 地址 212.115.112.31；在浏览器地址栏中输入 http://www.mymobilephone.com:8000 访问该网站，可知端口用的是 8000。

【问题 2】

【本地路径】是用于存放网页文件的路径。Windows Server 2003 操作系统安装在 D 盘中，默认情况下，【本地路径】为 D:\Inetpub\wwwroot。由表 2-9 知，网页存放位置为 E:\web，可知【本地路径】为 E:\web，而不是默认路径。

【问题 3】

首页文档为 mymobilephone.asp，为了使用户能正常访问该网站，需要将该文件放在“默认内容文档”的首位。操作方法是单击【添加】按钮，在【添加内容页】对话框中输入 mymobilephone.com，然后单击【确定】按钮，此时 mymobilephone.com 位于“默认内容文

档”的下端，选中该文档，单击【上移】按钮，将其上移至顶端。或依次删除 default.htm、default.asp、index.htm 三个文件，单击【添加】按钮，加入 mymobilephone.com 文件。

【问题 4】

屏蔽某些 IP 地址时，其他所有的均可访问，只需将这些 IP 地址排除即可。本题中要屏蔽的 IP 地址为 192.168.1.116。具体操作为：在【目录安全性】选项卡中单击【IP 地址和域名限制】选项区内的【编辑】按钮；弹出【IP 地址和域名限制】对话框，选中【授权访问】单选按钮，然后单击【添加】按钮，在弹出的【拒绝访问】对话框中加入 IP 地址 192.168.1.116，如图 2-67 所示。



图 2-67 【拒绝访问】对话框

【问题 5】

除了主目录以外还可以采用虚拟目录作为发布目录。虚拟目录可以在不影响现有网站的情况下，实现服务器磁盘空间的扩展。而且，虚拟目录可以与原有网站不在同一个文件夹，不在同一个磁盘驱动器，甚至不在同一台计算机上，但用户在访问网站时，却感觉不到任何区别。

答案：

【问题 1】

(1) 212.115.112.31　　(2) 8000

【问题 2】

(3) D　　(4) E:\web

【问题 3】

单击【添加】按钮，加入 mymobilephone.com 文件，上移至顶端。或依次删除已有的三个文件，单击【添加】按钮，加入 mymobilephone.com 文件。

【问题 4】

选中【授权访问】单选按钮，然后单击【添加】按钮，在弹出的【拒绝访问】对话框中加入 IP 地址 192.168.1.116。

【问题 5】

(5) C

例 2 阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2008 年 5 月下午试题三)

【说明】

Apache 是 Linux 系统中最常用的 Web 服务器，常用的客户端程序是 IE 浏览器。

【问题 1】(8 分)

Web 客户端与服务器共同遵守__(1)__协议，默认端口号是__(2)__，协作的过程是：Web 客户端在浏览器的地址栏输入__(3)__，连接到相应的 Web 服务器上并获得指定的 Web 文档，然后断开与 Web 服务器的连接，最后，Web 文档以__(4)__格式在客户端解释。

【问题 2】(2 分)

在 Linux 系统中配置 Apache 服务器，需要具有__(5)__权限，才可以运行 Apache 配置工具 rfapache。

A. root　　B. boot　　C. administrator　　D. user

【问题 3】(2 分)

虚拟主机是指在同一台服务器上实现多个__(6)__。

A. DHCP 服务　　B. DNS 服务

C. Web 站点　　D. Telnet 服务

【问题 4】(2 分)

“配置基于 IP 的虚拟主机，前提是服务器上必须要有多块物理网卡”，该论述是__(7)__的。

A. 正确　　B. 不正确

【问题 5】(1 分)

“如果服务器只有一个 IP 地址，用不同的端口号也能创建不同的虚拟主机”，该论述是__(8)__的。

A. 正确　　B. 不正确

分析：

【问题 1】

Web 服务是采用客户机/服务器模式，以超文本标记语言(HTML)与超文本传输协议(HTTP)为基础，为用户提供界面一致的信息浏览系统。在 Web 服务系统中，信息资源以页面的形式存储在服务器中，页面采用超文本方式对信息进行组织，通过链接将一页信息链接到另一页信息。页面到页面的连接信息由统一资源定位符(URL)维持，用户通过浏览器向 Web 服务器发出请求，服务器进行回应，将图文并茂的页面呈现给用户。

Web 服务器中的页面采用超文本标记语言(HTML)书写而成。HTML 可以定义格式化的文本、色彩、图像与超文本链接等，主要用于 WWW 页面的创建和制作。

Web 的服务器软件默认使用 TCP 80 端口监听，等待客户端浏览器发出的连接请求。连接建立后，客户端可以发出一定的命令，服务器给出相应的应答。

【问题 2】

rfapache 是 Apache Server 图形化配置工具。它根据 Apache Server 的特点，结合 Windows 系统管理员使用 IIS 的习惯，通过一个友好的交互界面。rfapache 配置工具需要在 KDE 环境下以 root 权限运行，非 root 用户虽然允许运行和使用配置工具，但由于没有权限修改配置文件，所以即使在配置工具中修改了选项也无法保存和生效。

【问题 3】

虚拟主机是指在一个单一的服务器上维护多个 Web 站点，并且使用主机别名来区别它们。这样就可以在单一的 Web 服务器上拥有多个 Web 站点，并通过它们各自的域名对这些站点进行访问。

【问题 4】

基于 IP 的虚拟主机用不同的 IP 地址来区分不同的虚拟网站。操作系统可以支持服务器上的每块网卡绑定多个不同 IP 地址，因此即便是服务器上只有一块物理网卡，也可以采用基于 IP 的虚拟主机策略。

【问题 5】

Web 服务的默认端口号是 80，但仍可以使用其他的端口号来配置新的 Web 服务，因此在基于 IP 的虚拟主机配置策略中，如果指定了 IP 地址和端口号，是可以有效区分 Web 虚拟站点的。

当 Web 请求达到服务器时，Web 服务器软件(Apache)用达到请求的 IP 地址和端口来发现匹配的虚拟主机配置，并用对应的虚拟服务器的配置来处理请求，因此可以用不同的端口号来创建虚拟主机。

答案：

【问题 1】

(1) HTTP(或超文本传输协议)

(2) 80

(3) IP 地址(或域名，或 URL)

(4) HTML(或超文本标记语言)

【问题 2】

(5) A

【问题 3】

(6) C

【问题 4】

(7) B

【问题 5】

(8) A

例 3　认真阅读下列有关 Linux 操作系统环境下配置 Apache 服务器的说明，根据要求回答问题 1～问题 7，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题四)

【说明】

一台装有 Red Flag Server 4.0 操作系统的计算机，该计算机的主机名是 webserver，所安装网卡上配置的 IP 地址、DNS 域名、用户主目录如表 2-10 所示。现在要把这台计算机用 rfapache 管理工具配置成一台 ApacheWeb 服务器。

表 2-10　某计算机的网卡配置

用 户 名	IP 地 址	DNS 域名	主 目 录
Corp	192.168.0.10	www.corp.com	/var/www/corp
Dept1	192.168.0.11	www.dept1.com	/var/www/dept1
Dept2	192.168.0.12	www.dqpt2.com	/var/www/dept2
Dept3	192.168.0.13	www.dept3.com	/var/www/dept3

续表

用 户 名	IP 地 址	DNS 域名	主 目 录
Dept4	192.168.0.14	www.dept4.com	/var/www/dept4
Dept5	192.168.0.15	www.dept5.com	/var/www/dept5
Dept6	192.168.0.16	www.dept6.com	/var/www/dept6

【问题 1】(2 分)

在 KDE 环境下运行 rfapache，若要完成 rfapache 的配置操作，需要用户具有___(1)___权限。

【问题 2】(2 分)

虚拟主机是指在一个单一的服务器上创建和维护多个 Web 站点，Apache 提供了对虚拟主机的完全支持。虚拟主机的形式可以是(2)、(3)。

(2)和(3)备选项如下：

A．基于名字　　D．基于文件　　C．基于 IP 地址　　D．基于 MAC 地址

【问题 3】(2 分)

图 2-68 是虚拟主机的站点属性设置界面，请填写用户 Dept5 的 Web 站点配置信息。

IP 地址：___(4)___；TCP 端口：___(5)___。



图 2-68　【站点属性】选项卡

【问题 4】(2 分)

如果 Dept5 的 Web 站点使用 8000 端口侦听 Web 服务请求，那么用户在浏览器的地址栏中输入___(6)___可以访问该站点。

【问题 5】(2 分)

图 2-69 是虚拟主机的主目录属性设置界面，给出用户 Dept5 的 Web 站点的主目录路径___(7)___。通常，Web 站点主文档的默认文件名为___(8)___。



图 2-69 【主目录】选项卡

【问题 6】(3 分)

图 2-70 是虚拟主机的访问控制属性设置界面。假设只允许 IP 地址范围是 192.168.1.1/24 的计算机访问用户 Dept5 的 Web 站点，请设置相应的属性配置参数。

“访问”(控制属性)：__(9)__。

A．允许　　　　B．禁止

“IP 地址/域名”(范围)从__(10)__～__(11)__。



图 2-70 【访问许可】选项卡

【问题 7】(2 分)

运行 rfapache 需要启动的守护进程是__(12)__。

分析：

本题主要考查 Red Flag Server 4.0 操作系统下 Apache Web 服务器的配置。

【问题 1】

rfapache 是 Red Flag Server 4.0 操作系统下 Apache Web 服务器的图形化配置工具，通过该工具可以修改 Apache 服务器的配置文件 httpd.conf，因此它需要在 KDE 环境下以 root 权限运行。尽管非 root 用户允许运行和使用该配置工具，但由于没有权限修改配置文件 httpd.conf，所以即使在配置工具中修改了配置参数也无法保存和生效。

【问题 2】

虚拟主机是指在一台 Web 服务器上，提供多个 Web 服务。在 Apache Web 服务器中，有两种设定虚拟主机的方式：一种是 IP-Based(基于 IP 方式)，另一种是 Name- Based(基于域名方式)。

【问题 3】

本题提供的虚拟主机是基于 IP 方式，Dept5 的 Web 站点的 IP 地址是 192.168.0.15。在默认情况下，Web 服务器通过监听 TCP 端口 80 来接收 Web 客户机的请求。

【问题 4】

TCP 端口号默认值为 80，也可以分配其他的端口号。如果这样做，访问 Apache 服务器时就必须在 URL 后面跟上端口号才能访问到页面，即 http://apacheserver:port。

【问题 5】

Dept5 的 Web 站点的主目录路径是/var/www/dept5。Web 站点的默认文档是指，当 URL 请求解析时是一个目录而没有文件名时，就用默认文档去响应客户机。为了方便区分默认文档，其文件名一般取 index.htm、default.htm、welcome.htm、index.php 等。

【问题 6】

在 Apache 服务器中，可以通过访问许可来限制某些用户的访问 Web 站点。通常有两种方法：第一种方法是设置成“允许”，并把要允许访问主机的 IP 地址范围或域名填入访问列表，这样只有列表中的主机可以访问该 Web 站点，其他主机都无法访问该 Web 站点；第二种方法是设置成“禁止”，并把要禁止访问主机的 IP 地址范围或域名填入访问列表，这样除列表中的主机不能访问该 Web 站点外，其他主机都可以访问该 Web 站点。很显然，本题是采用第一种方式，网络 192.168.1.1/24 中第一个可用 IP 地址是 192.168.1.1，最后一个可用 IP 地址是 192.168.1.254，192.168.1.0 和 192.168.1.255 分别代表该网络的网络地址和广播地址。

【问题 7】

rfapache 是 Apache Web 服务器的图形化配置工具，运行 rfapache 时需要启动 Web 服务器的守护进程，否则无法配置，而 Apache Web 服务器的守护进程是 httpd。

答案：

【问题 1】

(1) root

【问题 2】

(2)、(3)A、C 或 C、A

【问题3】

(4) 192.168.0.15

(5) 80

【问题4】

(6) http://www.dept5.com:8000 或 http://192.168.0.15:8000

【问题5】

(7) /var/www/dept5

(8) index.htm 或 default.htm 或 welcome.htm

【问题6】

(9) A

(10) 192.168.1.1

(11) 192.168.1.254

【问题7】

(12) httpd

2.5.3 同步练习

1．在 Red Flag Linux 中可以通过什么命令启动 Apache 配置工具？

2．在 Red Flag Linux 中如何启动 Apache 服务？请说出两种方式。

3．阅读以下说明，回答问题 1～问题 6，将答案填入对应的答案栏内。

【说明】

有一台 Linux 服务器，配置了 Apache 服务，该服务器运行于独立方式下，监听端口是 80，工作目录为/usr/local，主文件目录为/www/，用户文档目录为 public_html。当用户请求一个不存在的文档时，用文档/missing.html 来回应用户浏览器，建立了一个虚拟目录，需要建立一个虚拟目录/icons/，其真实路径是/var/www/icons。以下是 httpd.conf 配置文件的片段：

```
## httpd.conf -- Apache HTTP server configuration file
### Section 1: Global Environment
ServerType ______(1)______
ServerRoot "______(2)______"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MaxClients 150

### Section 2: 'Main' server configuration
Port 80
User apache
Group apache
ServerAdmin root@localhost
ServerName localhost
```

```
DocumentRoot "__________(3)__________"
UserDir public_html
DirectoryIndex index.html index.htm index.php index.php4
_____________(4)_____________
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument ____________(5)____________
```

【问题 1】(1)处填什么内容?

【问题 2】(2)处填什么内容?

【问题 3】(3)处填什么内容?

【问题 4】在(4)处需要建立一个名称为/icons/的虚拟目录，则应填什么内容?

【问题 5】(5)处填什么内容?

【问题 6】httpd.conf 文件中阴影一行的含义是什么?

2.5.4　同步练习参考答案

1．在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfapache。

2.

方法一：使用命令行终端来启动，命令如下。

```
#/etc/init.d/httpd start
```

方法二：使用菜单命令来启动　在控制台菜单中选择【操作】|【启动】命令。

3.

【问题 1】standalone

【问题 2】/usr/local

【问题 3】/www/

【问题 4】Alias /icons/ "/var/www/icons/"

【问题 5】404 /missing.htm

【问题 6】该行是指定索引文件(默认文档)及搜索顺序，即当用户访问一个目录时没有指定文件名时，依次寻找 index.htm、index.htm、index.php、index.php 文件，并用它来响应客户的请求。

2.6　代理服务器配置

2.6.1　考点辅导

2.6.1.1　代理服务器的基础知识

1. 代理服务器的概念和功能

随着 Internet 技术的迅速发展，越来越多的个人计算机接入了 Internet，很多公司也将

自己公司的局域网接入了 Internet。如何快速地访问 Internet 站点，提高网络的安全性，成为当今的热门话题。在这种情况下，代理服务器便应运而生了。

1) 代理服务器的概念

代理服务器(Proxy Server)是个人网络和 Internet 服务商之间的中间代理机构，它负责转发合法的网络信息，对转发进行控制和登记。代理服务器作为连接 Internet 与 Intranet 的桥梁，在实际应用中发挥着极其重要的作用。它可用于多个目的，最基本的功能是连接，此外还提供安全性、缓存、内容过滤、访问控制管理等功能。代理服务器，顾名思义，就是代理网络服务的机构。局域网上不能直接上网的电脑将上网请求(如浏览某个主页)发给能够直接上网的代理服务器，由代理服务器代理完成这个上网请求，将请求者所要浏览的主页调入代理服务器的缓存；然后将这个页面传给请求者。这样，局域网上的电脑就如同能够直接访问网络一样。并且，代理服务器还可以进行一些网站的过滤和控制工作，这样就实现了控制和节省上网费用的目的。

代理服务器能够让多台没有 IP 地址的电脑利用其代理功能高速、安全地访问互联网资源。当代理服务器客户端发出一个对外的资源访问请求后，该请求先被代理服务器识别并代为向外请求访问资源。由于一般代理服务器拥有较大的带宽、较高的性能，并且能够智能化地缓存已浏览或未浏览的网站内容，因此，在一定条件下，客户端通过代理服务器能更快速地访问网络资源。代理服务器应用的常见例子：拥有上百台电脑的局域网通过一台能够访问外部网络资源的代理服务器访问外部互联网。

2) 代理服务器的功能

(1) 作为防火墙

代理服务器可以保护局域网的安全，起防火墙的作用。通过设置防火墙，为公司内部的网络提供安全边界，防止外界的入侵。

(2) 实现网络地址转换

网络地址转换(Network Address Translation，NAT)最主要的功能是实现 IP 地址的多个对应多个或者多个对应一个的映射，从而节约 IP 地址空间。基于这种功能，通过代理服务器访问 Internet 便可以解决合法的 IP 地址不够用的问题。公司局域网的用户通过代理服务器访问外界时，可以只映射一个 IP 地址，这样公司就不必租用多个 IP 地址了。

(3) 网址过滤和访问权限限制

代理服务器可以设置 IP 地址过滤功能，对外界或内部的 Internet 地址进行过滤，限制不同用户的访问权限。例如，代理服务器可以用来限制封锁 IP 地址，禁止用户浏览某些网页。

(4) 提高访问速度

代理服务器将远程服务器提供的数据保存在自己的硬盘上，如果有许多用户同时使用这一个代理服务器，当有人访问过某一站点后，所访问站点的内容便会被保存在代理服务器的硬盘上，如果下一次再要访问这个站点时，这些内容便会直接从代理服务器磁盘中取得，而不必再次连接到远程服务器上获取。因此，使用代理服务器可以节约带宽、提高访问速度。

2. 代理服务器的工作原理

代理服务器的工作原理是：当用户在浏览器中设置好代理服务器后，使用浏览器访问

所有 Web 站点的请求都不会直接发送给目的主机，而是先发送给代理服务器，代理服务器接受了用户的请求以后，向目的主机发出请求，并接收目的主机的数据，存于代理服务器的硬盘中，然后再将用户要求的数据发给用户。

下面来详细说明其工作过程。

当用户端对服务器端提出请求时，此请求会被发送到代理服务器，然后代理服务器会检查本身是否有用户端所需要的数据。如果有而且没有过期，代理服务器便代替服务器将数据传给用户端。而用户端一般会选择距自己传输距离较近的某台代理服务器，所以从代理服务器申请得到数据的速度可能会比从远程服务器申请数据要快。

如果代理服务器没有用户端所请求的数据或数据已经过期，它会去服务器获取所需的数据。在代理服务器从服务器端取得数据传给用户端时，自己保存一份，待下次如果有用户提出相同的请求时，便可以将数据直接传过去，而不需要再去服务器端获取了，如图 2-71 所示。

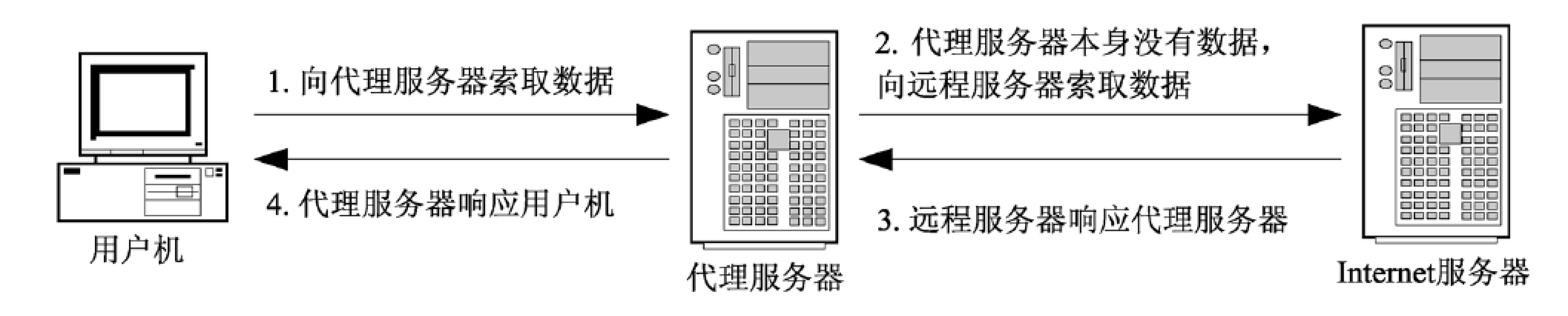


图 2-71　代理服务器工作原理示意

3. 代理服务器的架设

代理服务器在运行方式上可以分为透明代理和传统代理两类。下面介绍的 WinGate 代理服务器既可以作透明代理，也可以作传统代理。但对于这两种代理方式，用户端的网络设置和软件设置并不相同。下面以一个例子来说明两种代理用户机的设置方式。

假如某公司向 ISP 申请了 ADSL 业务以接入 Internet，相关参数为：IP 地址为 220.102.168.10、子网掩码为 255.255.255.248、默认网关为 220.102.168.10、DNS 为 202.102.192.68。现通过一台代理服务器，实现整个公司用户访问 Internet。

1) 代理服务器的网络设置

(1) 安装硬件。在代理服务器中安装一块 ADSL 接口卡用于接入 Internet，安装一块网卡用于接入公司内部局域网。

(2) 设置 ASDL 接口卡网络参数。IP 地址为 220.102.168.10、子网掩码为 255.255.255.248、默认网关为 220.102.168.10、DNS 为 202.102.192.68，如图 2-72 所示。访问 Internet 看是否能正常访问，如能访问，则说明接入 Internet 已经设置好了。

(3) 设置网卡的网络参数。假设局域网使用配置 192.168.1.0/24 这个 C 类地址，使用它的第一个 IP 地址(192.168.1.1)作为该网卡的 IP 地址，子网掩码为 255.255.255.0，其他参数可以不设置。

(4) 安装代理服务器软件，并进行相关配置。

通过上面 4 个步骤，代理服务器基本设置完毕。

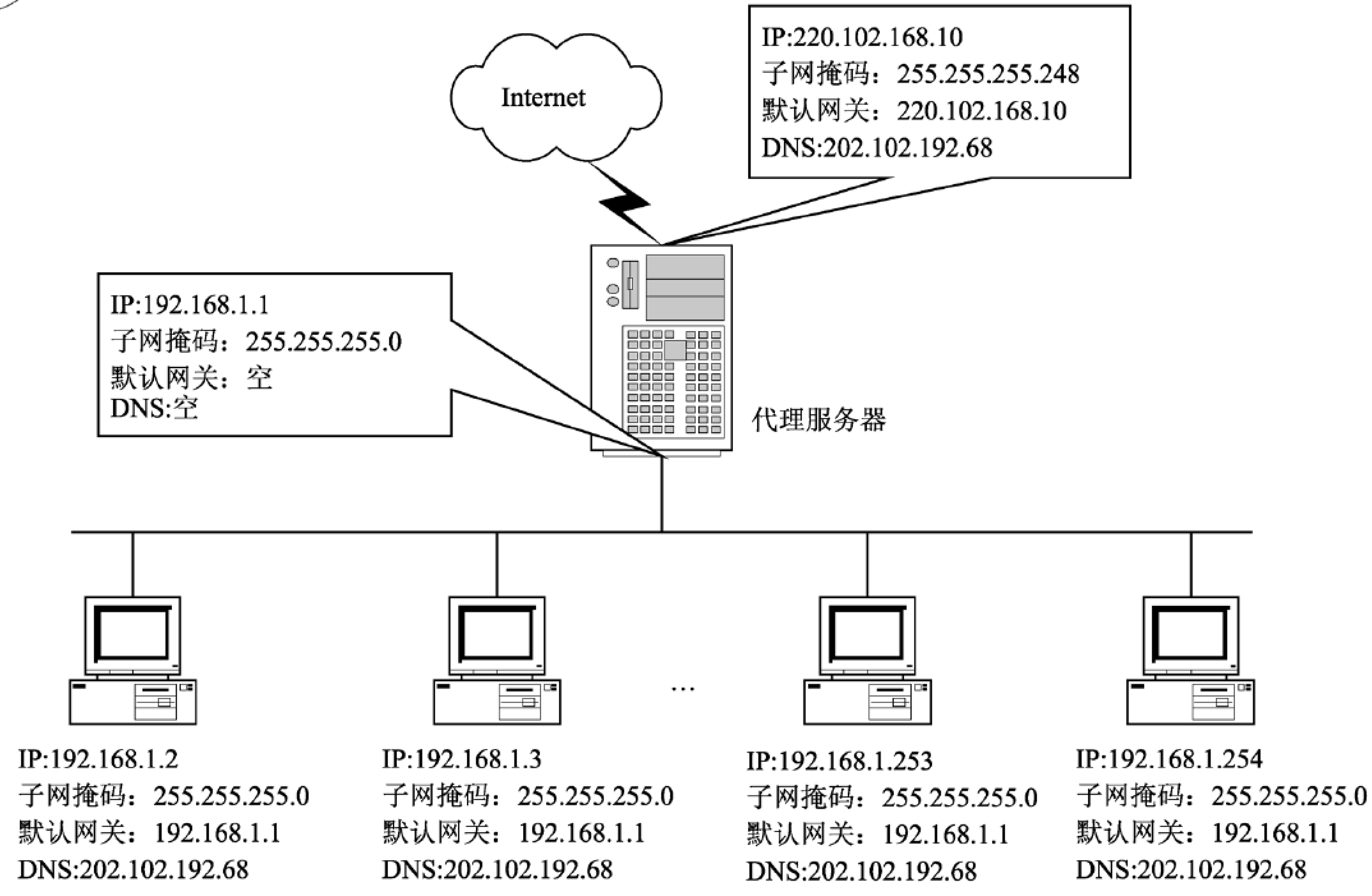


图 2-72　透明代理的网络配置

2)　用户机的网络设置

(1)　透明代理

透明代理的意思是用户端根本不需要知道有代理服务器的存在，用户机好像就直接连接到 Internet 上。用户端需作如下设置：一是设置网络参数，包括 IP 地址(范围为 192.168.1.2～192.168.1.254)、默认网关为 192.168.1.1、DNS 为 202.102.192.68，如图 2-72 所示。二是安装用户端软件并做相应设置。

(2)　传统代理

在传统代理中，用户端网络设置比较简单，只需要设置 IP 地址就可以了，不需要安装用户端软件。在这个例子中，用户端 IP 地址设置范围为 192.168.1.2～192.168.1.254，默认路由、DNS 都可以不设置。但在应用软件上(如 IE、QQ、CuteFTP 等)必须要做相应设置，主要有两个参数：一个是代理服务器的 IP 地址(本例中设为 192.168.1.1)，另一个是端口号，对于不同服务端口号可能不同。

不论是采用透明代理还是传统代用，客户机的参数都可以通过 DHCP(动态主机分配协议)来动态分配 IP 地址和相关参数，这样可以简化网络管理。

2.6.1.2　WinGate 代理服务器的配置

1.　WinGate 服务器端的基本设置

(1)　设置 WinGate 管理员密码。WinGate 安装成功后，每次启动计算机都会自动运行，并在任务栏生成一个 WinGate 的图标 CH 0:22 。双击该图标，要求输入 WinGate 管理员的密码，由于刚安装 WinGate，未设置密码，单击 OK 按钮即可，如图 2-73 所示。然后 WinGate

弹出对话窗口，提示为了系统的安全，必须设置密码。单击 OK 按钮，弹出 Set Administrator Password 对话框，在 New Password 和 Confirm New 文本框中输入相同的密码，单击 OK 按钮。

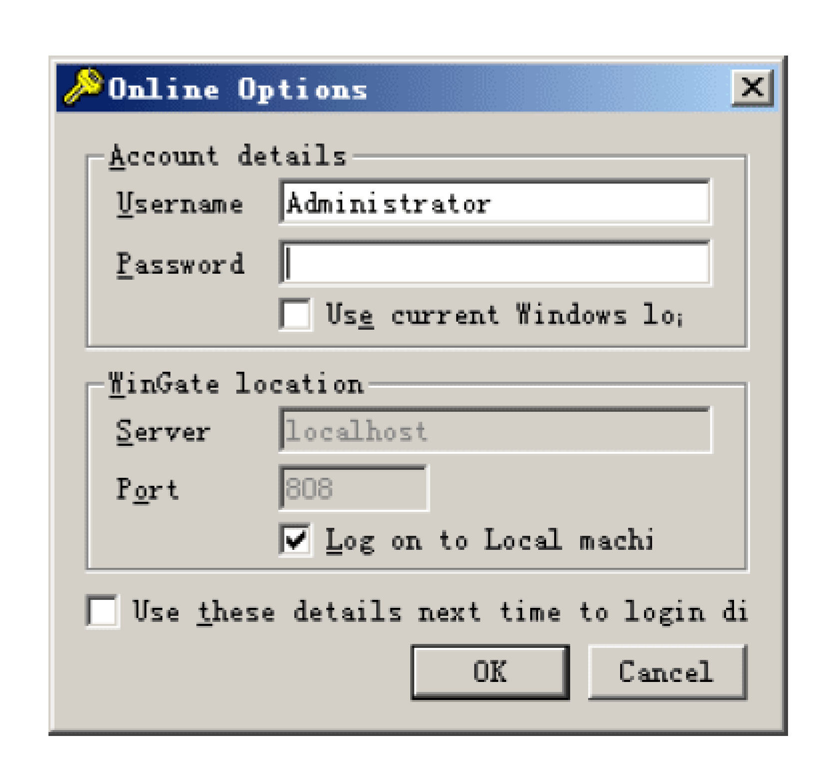


图 2-73　WinGate 服务器登录对话框

(2) 认识 WinGate 管理主界面。双击任务栏上的 WinGate 图标，输入管理员密码，进入 WinGate 的管理主界面，如图 2-74 所示。WinGate 管理主界面主要分两大块：左边为系统设置，右边为消息显示。System 选项卡主要用来设置 WinGate 的核心服务，如 DHCP 服务、DNS 服务、Caching 的设置、DNS 扩展网络支持的管理等。一般来说，WinGate 的默认设置就已经可以很好地工作了，无须做太多的修改。Services 选项卡用于设置 WinGate 代理服务的核心，如 Web 服务，Socks 服务，SMTP、POP3 服务等。Users 选项卡用于添加设置用户权限、用户组等。Activity 选项卡用于显示 WinGate 的运行状态。History 选项卡用于记录用户最近访问过的网站。System Messages 选项卡用于对 WinGate 系统信息的管理。由于 System、Services 的各项服务基本上可采取 WinGate 的默认设置值，这里主要是对帐户进行管理。

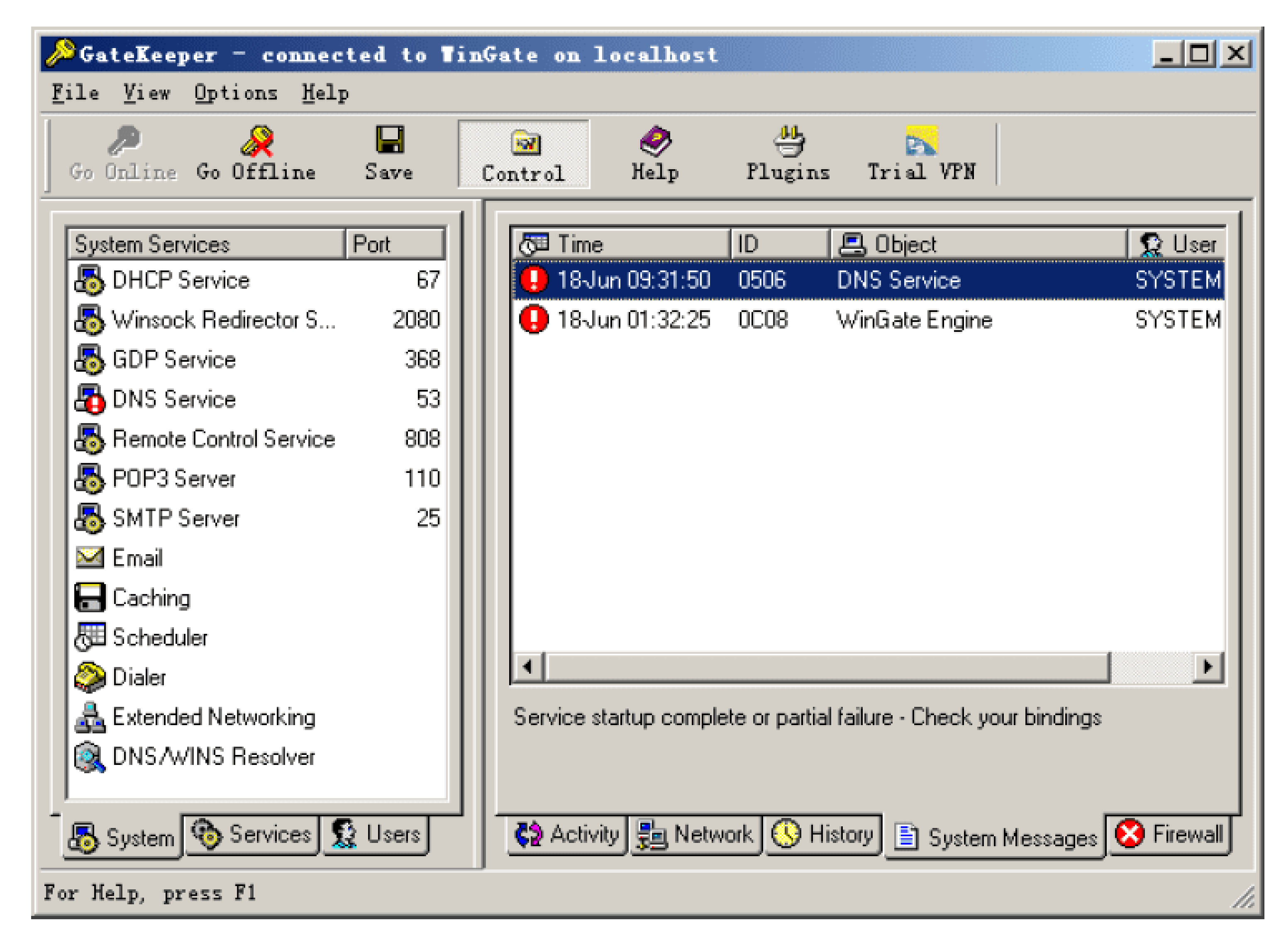


图 2-74　WinGate 的管理主界面

(3) 新建帐户。WinGate 对各个客户端进行管理，实际上大部分是通过对帐户进行管理实现的，以新建 zhang 帐户为例，介绍怎样新建一个帐户。具体操作步骤为：进入 WinGate 管理主界面，切换到 Users 选项卡，右击 Users 选项，在弹出的快捷菜单中选中 New User 选项，弹出 Properties for new user 对话框，如图 2-75 所示；切换到 User Info 选项卡，在 Username 文本框中输入 zhang，在 Real name 文本框中输入 zhangwurong，在 Password 和 Confirm 文本框中输入相同的密码，单击 OK 按钮即可。

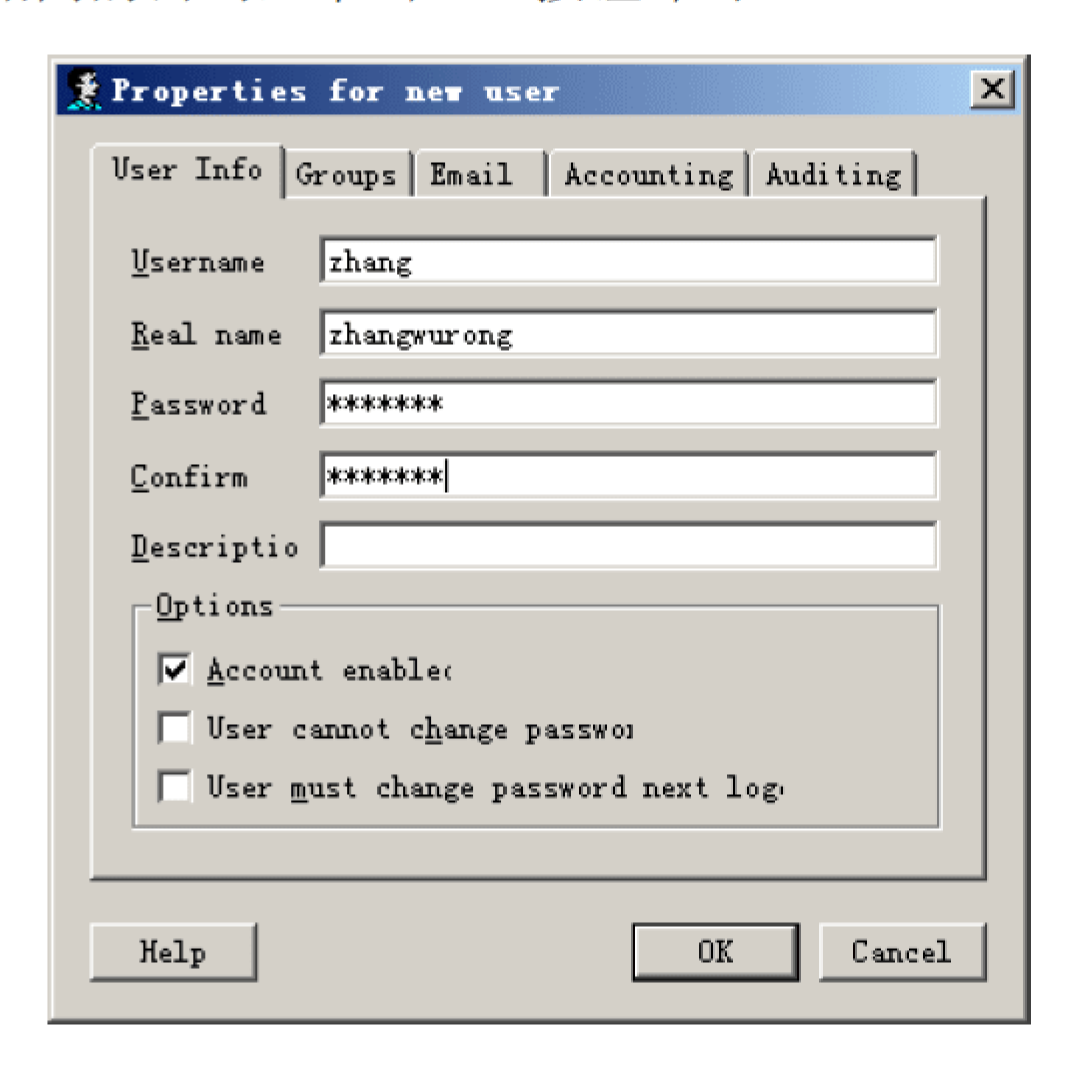


图 2-75 新建帐户

(4) 新建用户组。组就是将多个帐户统一管理，赋予其相同的权限，以新建 teachers 组为例，并将 zhang、tao 两个帐户添加至该组，介绍怎样创建一个用户组，并将帐户添加到组。操作步骤是：右击 Groups 选项，在弹出的快捷菜单中选择 New Groups 命令，弹出 New Group 对话框，如图 2-76 所示；在 Group Name 文本框中输入组名 teachers，然后在 Members 列表中选择 zhang、tao，单击 Add 按钮，将这些用户添加到该组。

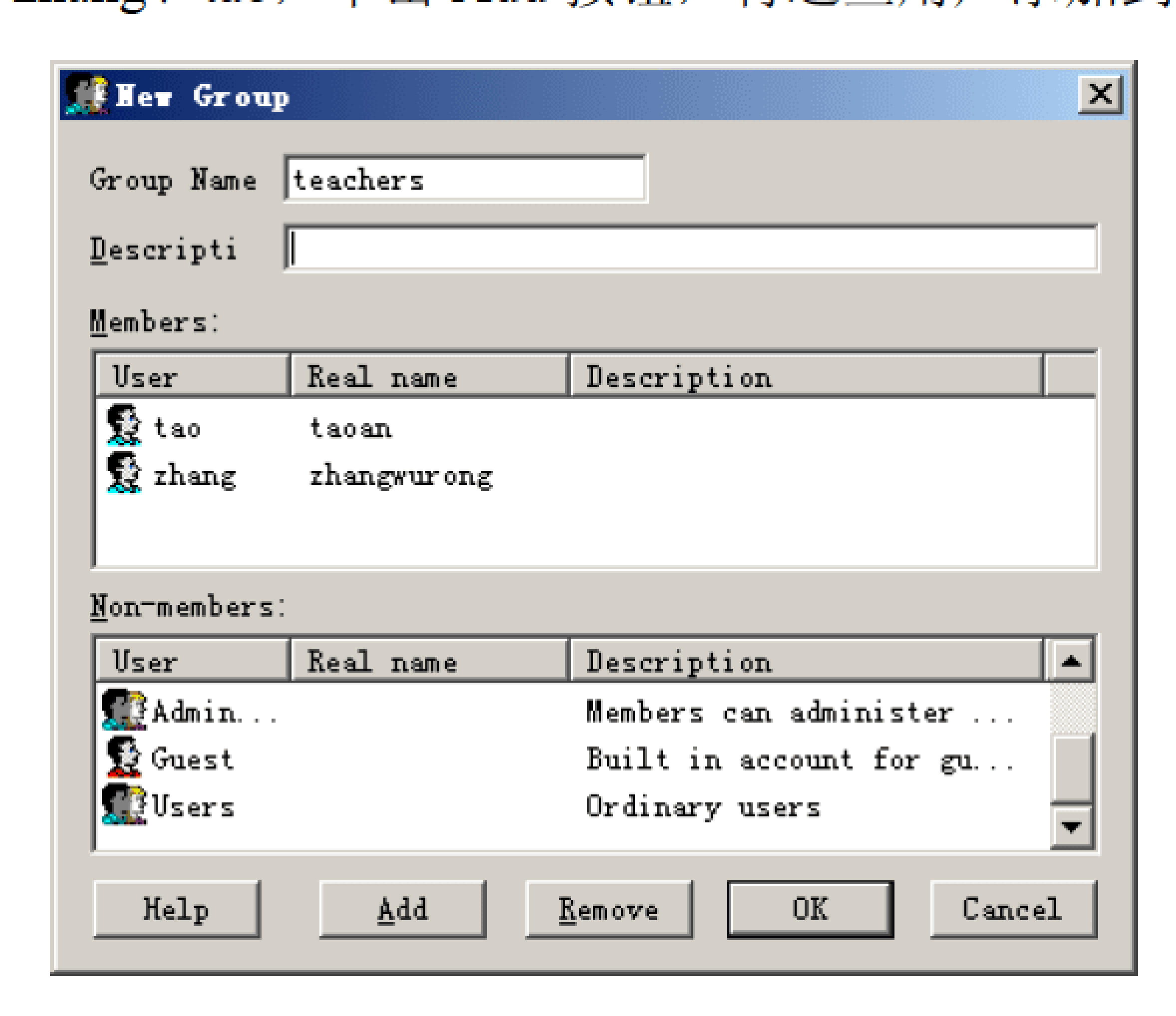


图 2-76 新建用户组

(5) 指定用户名与计算机的对应关系。创建用户与组后，需要将用户与计算机建立对

应关系，才能更好地进行管理，这里将以 zhang 与 IP 地址为 192.168.10.168 的计算机建立相对应的关系为例进行介绍。操作步骤为：在 WinGate 管理主界面，切换到 Users 选项卡，然后双击 Assumed Users 选项，弹出 Assumed users 对话框，如图 2-77 所示；用户与计算机建立对应关系，可以与计算机名或计算机的 IP 地址建立对应关系，为方便管理，一般是与 IP 地址建立相对应的关系；单击 Add 按钮，弹出 Add Users 对话框，在 if a user connects from IP address 文本框中输入与之对应的 IP 地址 192.168.10.168，在 Then assume it 下拉列表框中选择 zhang，单击 OK 按钮。用同样的方法将 tao 与 192.168.10.168 建立对应关系，单击 OK 按钮。

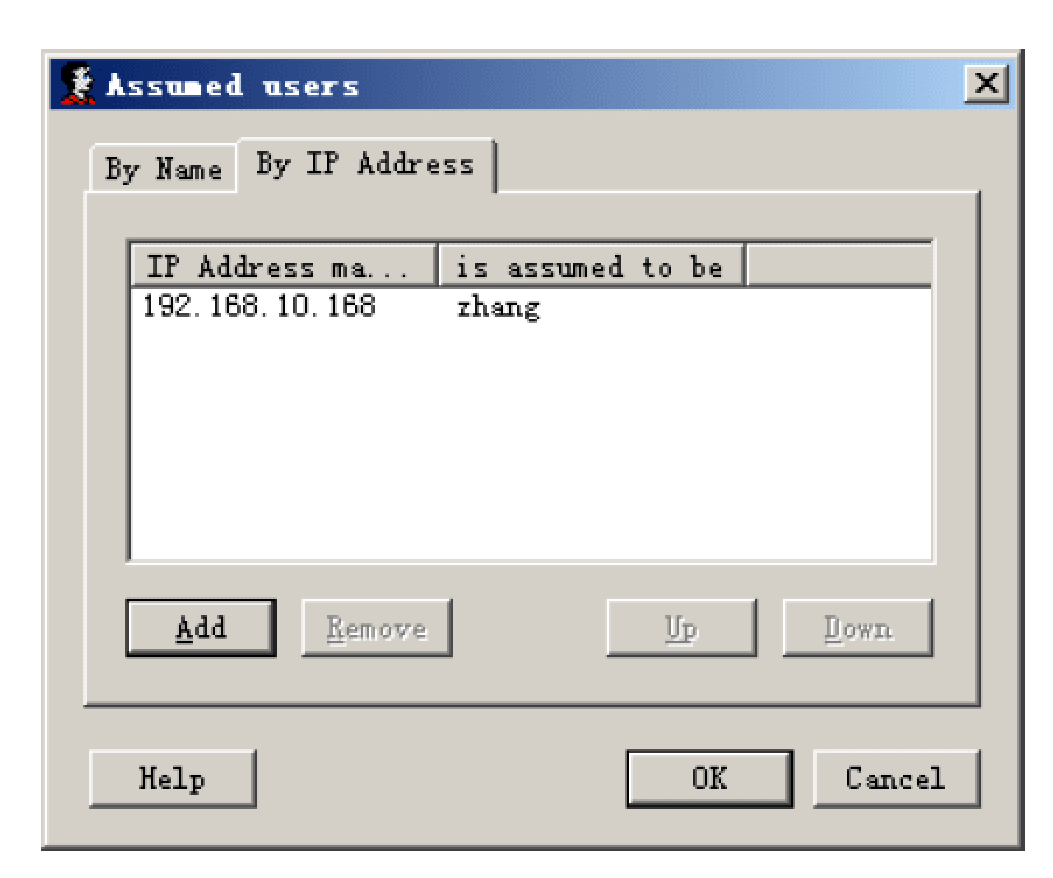


图 2-77　用户名与计算机的对应

(6) 限制只有注册用户才能访问 Internet。WinGate 的默认状态是启用 guest 帐户，客户端无须登录，只需设好代理地址，即可通过 WinGate 代理上网，如何限制只有授权用户才能访问 Internet 呢？操作步骤为：进入 WinGate 管理主界面，切换到 Users 选项卡，双击 System Policies 选项，弹出 Properties for recipient Everyone 对话框，如图 2-78 所示；在弹出的窗口中双击 Everyone 用户，在弹出的对话框中切换到 Recipient 选项卡，选中 User may be assume 单选按钮，单击 OK 按钮即可。

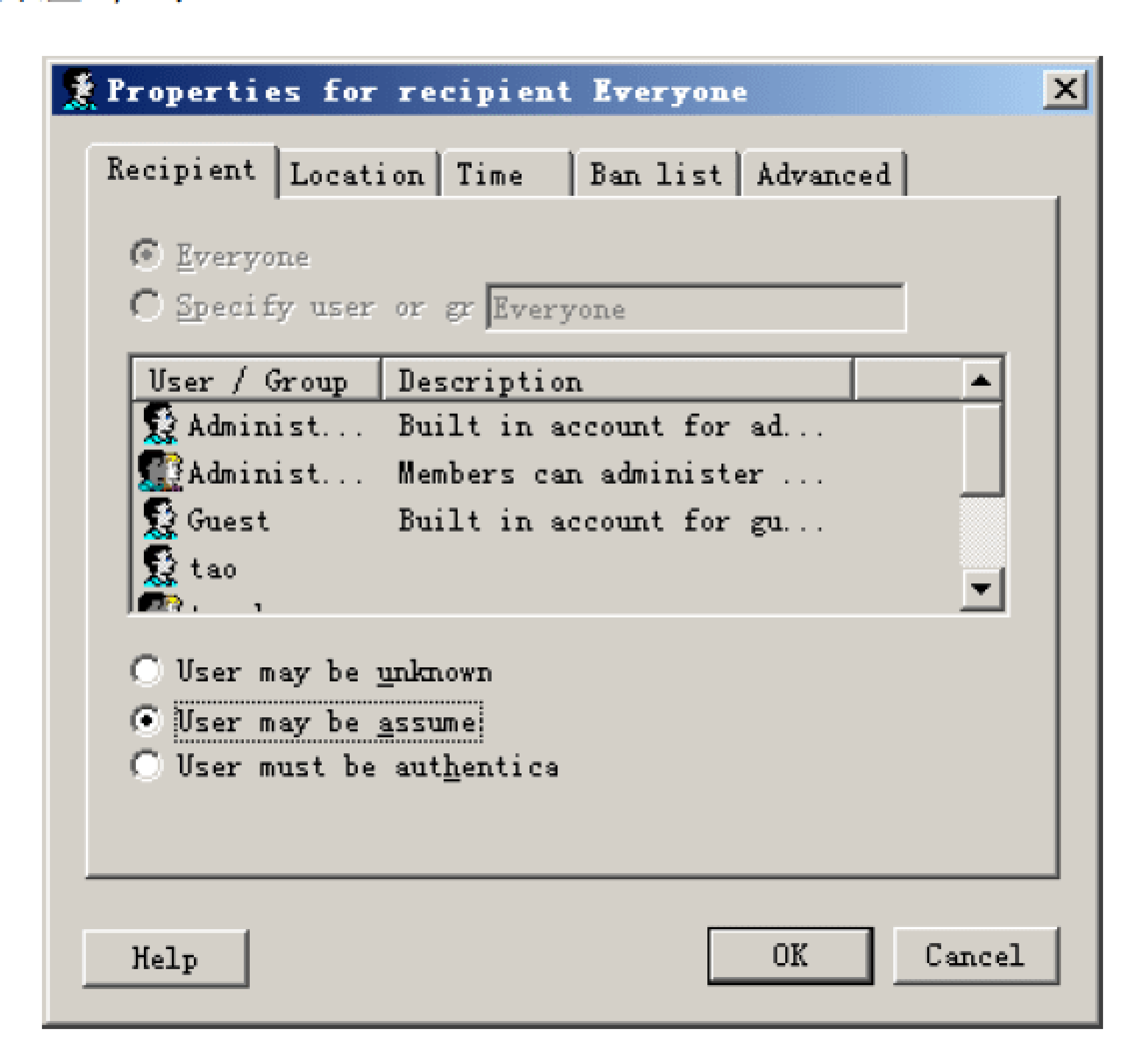


图 2-78　限制非注册用户的访问

(7) 限制访问网站。在管理 WinGate 的过程中，有时需要对网站的内容进行过滤，有不良信息则禁止访问。WinGate 默认设置没有任何限制，要实现这些功能，需要对设置进行修改。具体操作步骤如下：进入 WinGate 管理主界面，切换到 Services 选项卡，双击 WWW Proxy server 选项，弹出 WWW Proxy server properties 对话框，如图 2-79 所示；切换到 Policies 选项卡，将 Default rights 的选项改为 are ignored，表示非窗口列中允许的用户权限均不能访问；单击 Add 按钮，弹出 Properties for new recipient 对话框，如图 2-80 所示。然后切换到 Ban list 选项卡，单击 Add 按钮，弹出 Criterion 对话框，这个对话框其实就是一个规则表达式，数据来源可以为服务器域名、服务器 IP 和服务器 URL，规则表达式可以是等于或包含某些特定字符串，或以特定的字符串开始或结尾。把来源设为 HTTP URL，规则设为 contains(包含)，限制字符串输入“sex”，则表示不准当前用户访问包含 sex 的网站。最后单击 OK 按钮。重复上一步，将需要禁止访问的网站添加进来，可以是关键字，也可以是网站的 URL 全称。

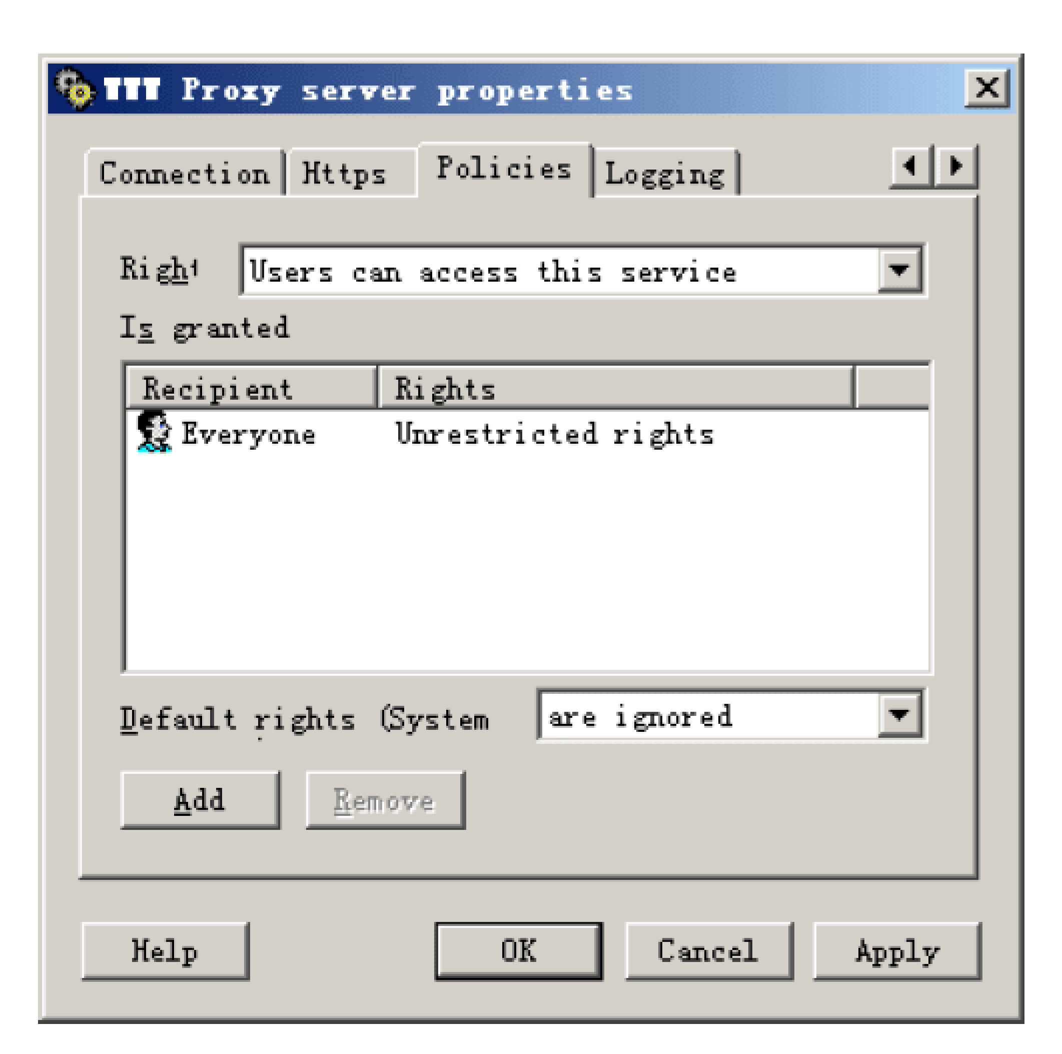


图 2-79　WWW Proxy server properties 对话框

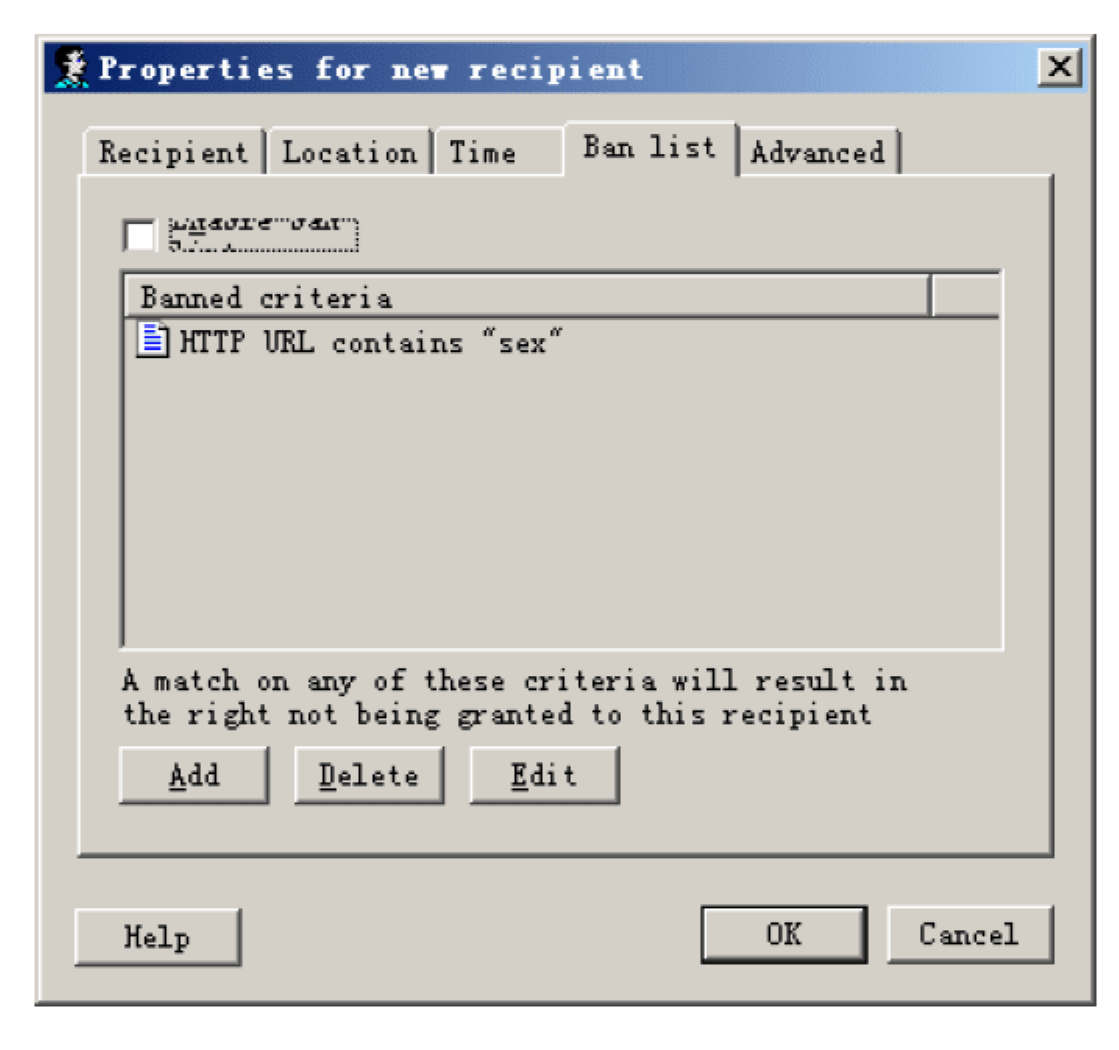


图 2-80　禁止访问包含“sex”的 URL

(8) 限制下载文件。有时为了节省带宽，不希望客户端下载文件，WinGate 为我们提供了禁用下载文件的方法，具体操作步骤如下：进入 WinGate 管理主界面，切换到 Services 选项卡，双击 WWW Proxy server，弹出 WWW Proxy server properties 对话框；切换到 Policies 选项卡。将 Default right 的选项改为 are ignored，表示非窗口列中允许的用户权限均不能访问；单击 Add 按钮，弹出 Properties for new recipient 对话框，然后切换到 Ban list 选项卡；单击 Add 按钮，弹出 Criterion 对话框，如图 2-81 所示，将表达式改为 HTTP URL、ends with、zip 即可，这表示不准用户下载以.zip 为扩展名的文件；重复上一步也可以将.rar、.exe、.cab、.iso、.img 等文件进行限制下载。

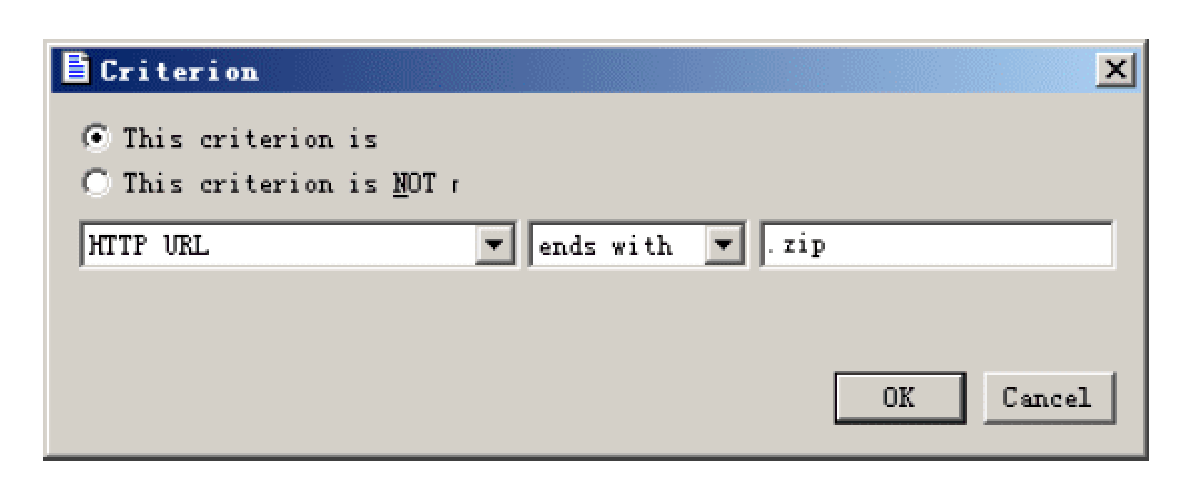


图 2-81　禁止下载以.zip 为扩展名的文件

(9) 指定浏览时间。操作步骤是：进入 WinGate 管理主界面，切换到 Services 选项卡，双击 WWW Proxy server，弹出 WWW Proxy server properties 对话框；切换到 Policies 选项卡，将 Default right 的选项改为 are ignored，表示非窗口列中允许的用户权限均不能访问；单击 Add 按钮，弹出 Properties for new recipient 对话框，然后切换到 Time 选项卡；单击 Specify times when this recipient has right 选项按钮，可以看到 Time 选项卡下有 Included times 和 Excluded time 列表框，Included times 列表框是设置允许使用时间段，系统到时会自动开启服务，而 Excluded time 列表框则是设置拒绝使用时间段，到时会自动关闭服务。若设置拒绝时间段，单击 Excluded time 列表框的 Add 按钮，弹出 Time Slice 对话框，如图 2-82 所示。在该对话框设置拒绝时间段，单击 OK 按钮。使用同样的方法，可设置允许使用时间段。

(10) 禁用 WinGate 的 DHCP 功能。有时候客户端自动获取的 IP 地址与 Windows 2000 服务器所设置的不一样(这里包括网关、DNS 等信息)，但进入 Windows 2000 的 DHCP 服务下查看却未查出是什么问题。其实问题所在是启用了 WinGate 的 DHCP 服务，同一子网有两个 DHCP 服务器，造成相互之间争抢资源的现象。解决的方法是禁用 WinGate 的 DHCP 功能。具体操作方法是：进入 WinGate 管理主界面，切换到 System 选项卡，双击 DHCP Service 选项，弹出如图 2-83 所示的对话框。切换到 General 选项卡，在该选项卡的 Start options 子选项的 Service 下拉列表中选择 Service is disabled，禁止使用 DHCP 服务，单击 OK 按钮。

(11) 设置缓存的大小。WinGate 可以对网页文件及其他文件进行缓存。缓存的大小需要合理配置，缓存过小会影响访问速度，过大则会对系统的稳定性产生影响。WinGate 默认缓存大小为 200MB，一般设置成 100～150MB 比较合适。修改缓存的具体操作步骤如下：进入 WinGate 管理主界面，切换到 Services 选项卡，单击 Caching 按钮，弹出 Cache Properties 对话框，如图 2-84 所示。在 Limit cache size 文本框中，将 200 修改为 150，单位是 MB，将第一个 Number of days before rechecking 改为 2，第二个 Number of days before rechecking 修改为 10。

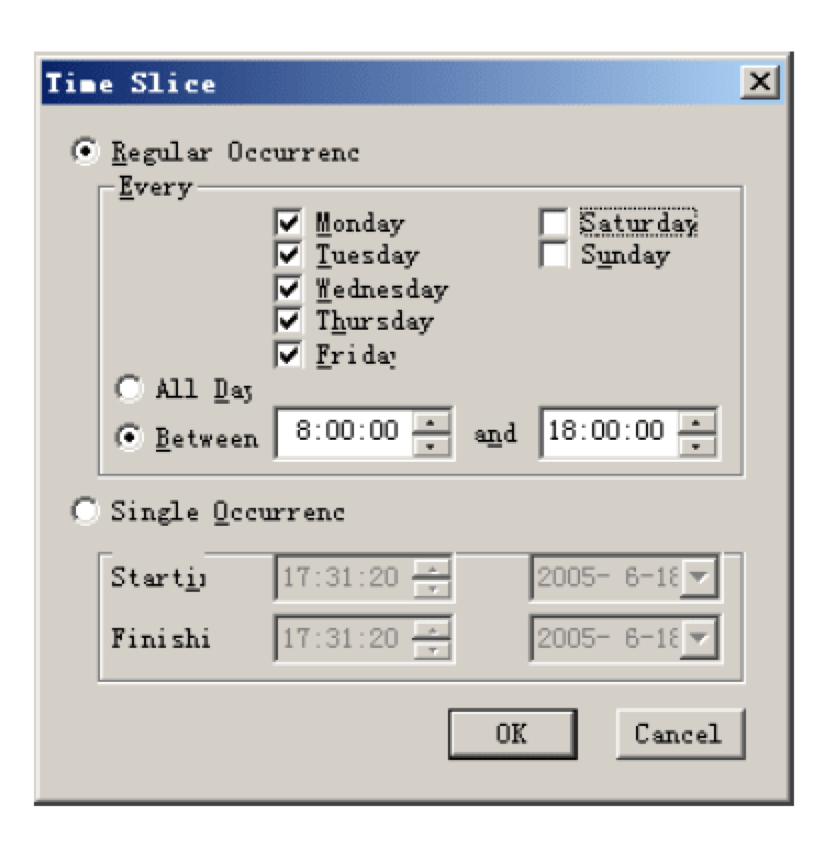


图 2-82　指定浏览时间

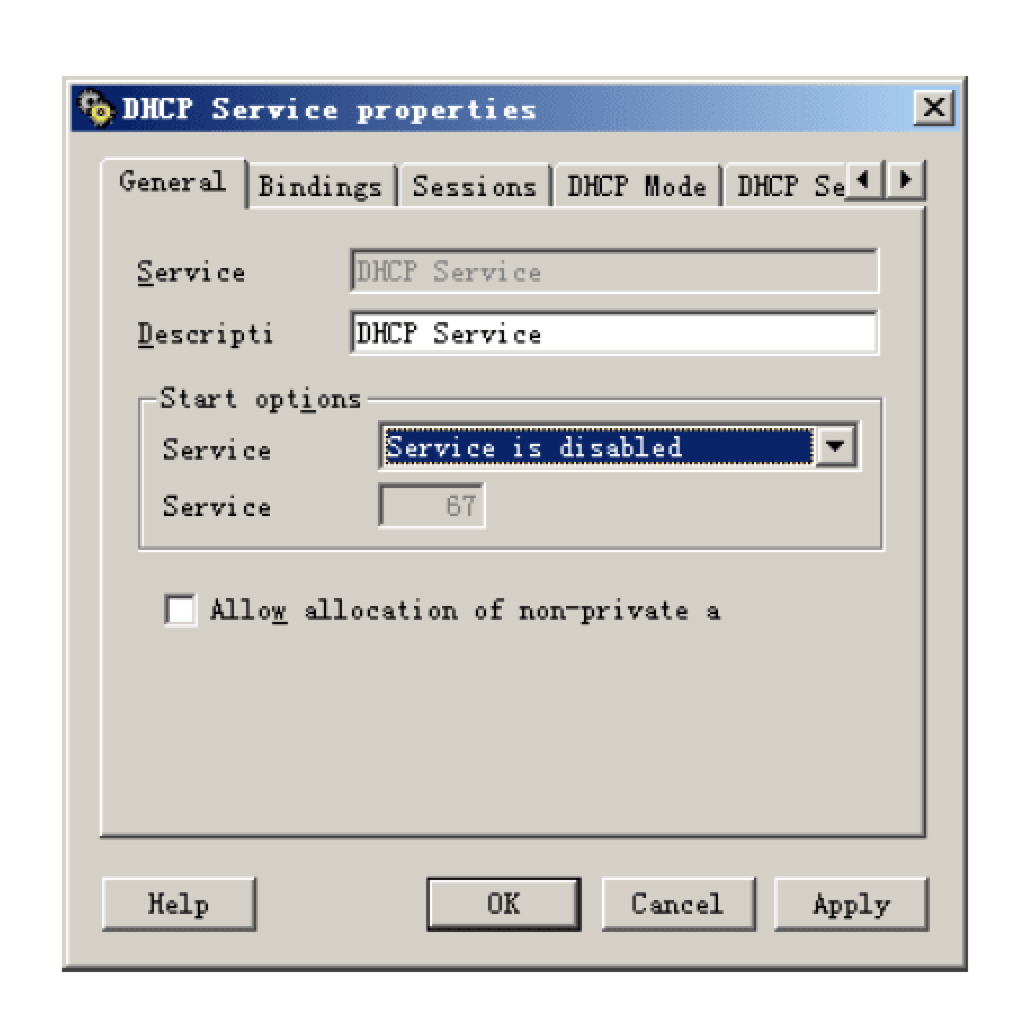


图 2-83　禁用 WinGate 的 DHCP 功能

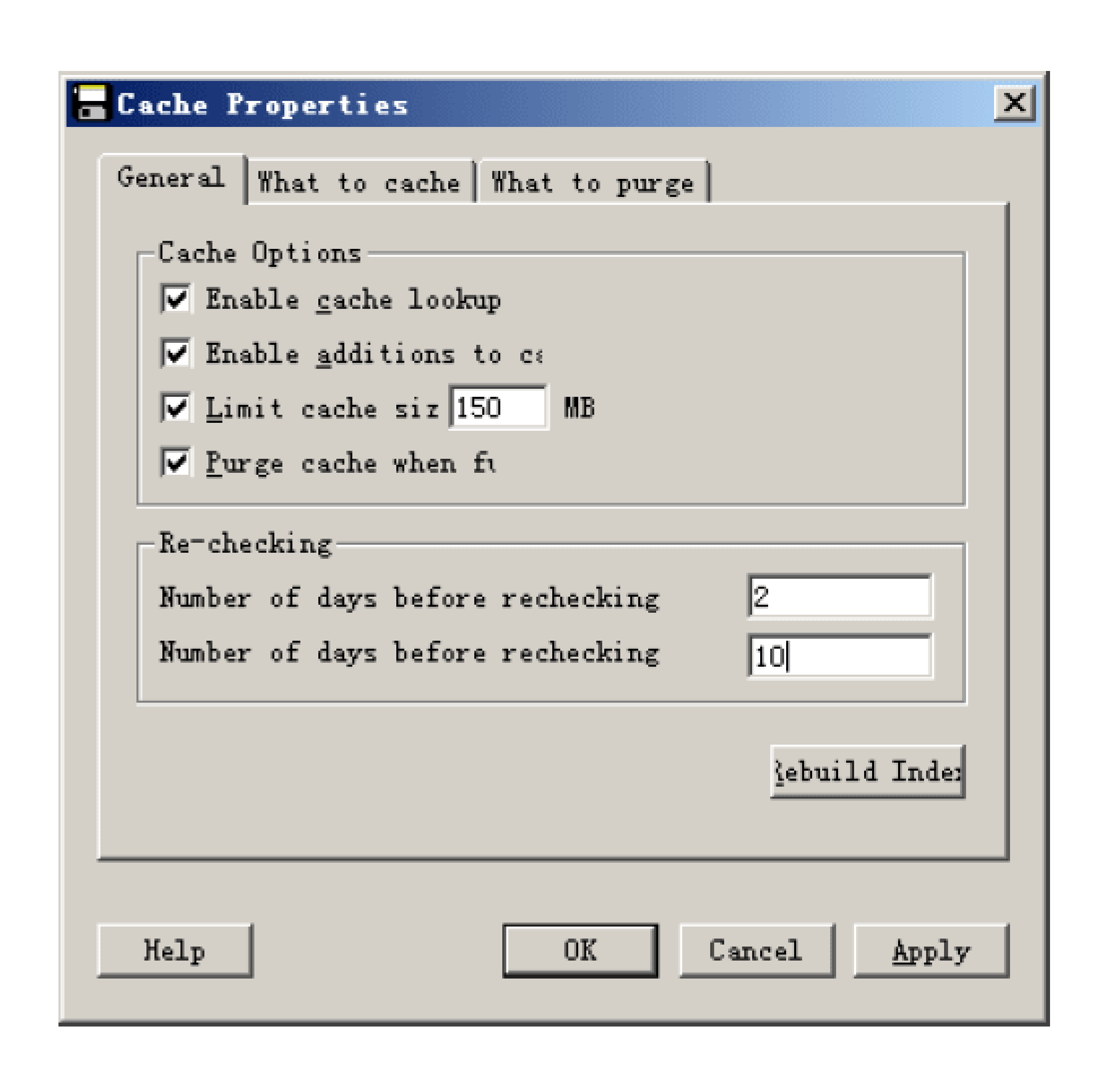


图 2-84　设置 WinGate 缓存的大小

2. 配置 WinGate 客户端

WinGate 既可工作在透明代理方式之下，也可工作在传统代理方式之下。因此，客户端使用 WinGate 服务器有两种配置方法：一种是安装 WinGate 客户端软件(透明代理方式)，另一种是直接对各个客户应用进行设置(传统代理方式)。下面分别介绍这两种代理方式。

1)　透明代理方式

这要求在每一台客户机上安装 WinGate 客户端软件，这样客户端软件会自动搜寻到 WinGate 服务器，所有客户端网络应用均不需作任何设置，就像直接连接到网络上一样方便。其操作步骤如下。

(1)　设置网关。

要将此客户机的网关设成 WinGate 服务器的内部局域网 IP 地址。

(2)　安装 WinGate 客户端软件。

WinGate 客户端软件和服务器安装相似，只是在上述的第(3)步中，选择 Configure this Computer as a WinGate Internet Client，然后同上面的安装步骤继续安装下去即可。

(3)　WinGate 客户端软件的设置。

在 WinGate 客户端软件安装完后，选择【开始】|【程序】| WinGate Internet Client | WinGate Internet Client Applet 命令，打开 WinGate Internet Client 对话框。切换到 General(常规)选项卡，选中 Enable the WinGate Internet Client 复选框，如图 2-85 所示，即可激活客户端，其他可不作设置。

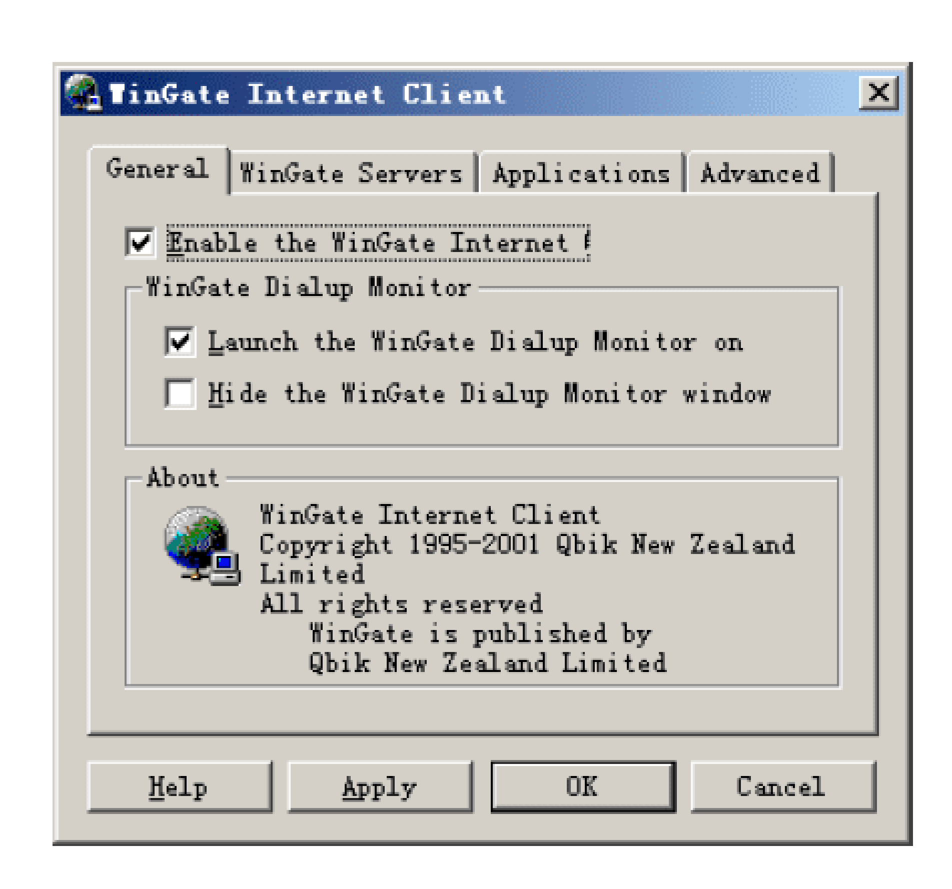


图 2-85　WinGate 客户端软件的设置

2)　传统代理方式

传统代理方式的好处是不需要安装客户端软件，在客户端应用软件上直接进行设置即可访问 Internet。

下面是一些常用客户端应用软件的设置。

(1)　Microsoft Internet Explore (IE)

打开【控制面板】|【Internet 连接】|【局域网设置】命令，在弹出的对话框中进行设置。选中【使用代理服务器】复选框，在【地址】文本框中输入 WinGate 服务器的内部局域网 IP 地址，【端口】文本框中输入 80，单击【确定】按钮。如果要进行具体设置，可切换到【高级】选项卡，即可对服务进行设置，如图 2-86 所示。

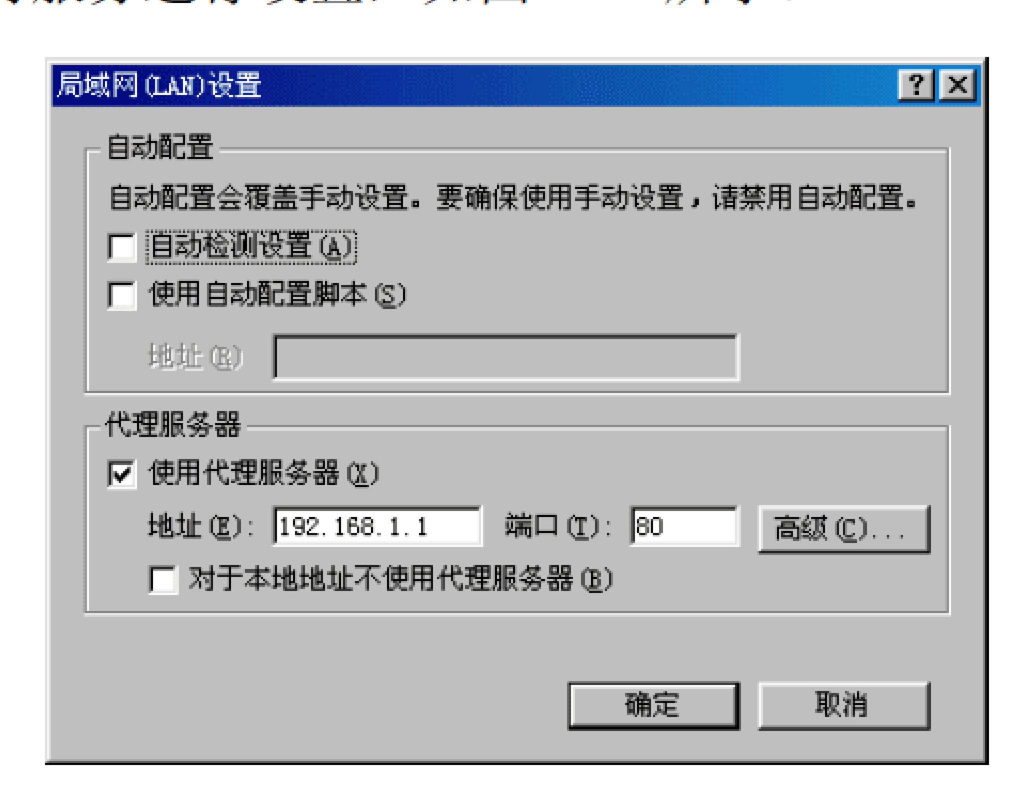


图 2-86　IE 浏览器代理服务器的设置

(2) Netscape

选择 Netscape 后，在菜单中选择 Edit | Preferences 命令，打开 Netscape 系统设置对话框，选择 Advanced | Proxies 命令，选中 Manual Proxy Configuration 单选按钮，单击 View 按钮后将弹出手工设置代理服务器对话框，如图 2-87 所示。在弹出的对话框中输入以下内容。

HTTP：WinGate 服务器的内部局域网 IP 地址，Port 为 80。

FTP：WinGate 服务器的内部局域网 IP 地址，Port 为 21。

Socks：WinGate 服务器的内部局域网 IP 地址，Port 为 1080。

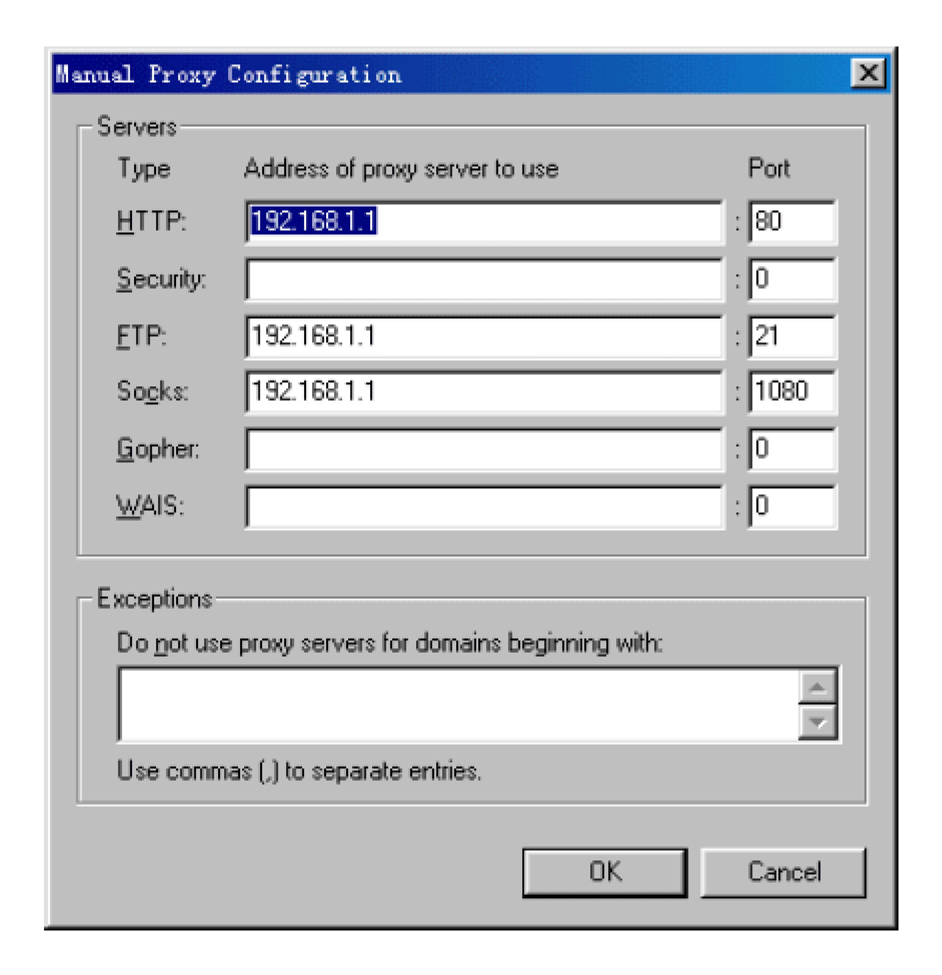


图 2-87 Netscape 浏览器代理服务器的设置

(3) CuteFTP

打开 CuteFTP 后，在主菜单中选择 Edit | Settings 命令，然后在弹出的对话框中选择 Connection | Socks 目录进行设置，如图 2-88 所示。

在图 2-88 中，选中 Socks 5 单选按钮，在 Host 文本框中输入 WinGate 服务器的内部局域网 IP 地址；Port 文本框中输入 1080，最后单击 OK 按钮。

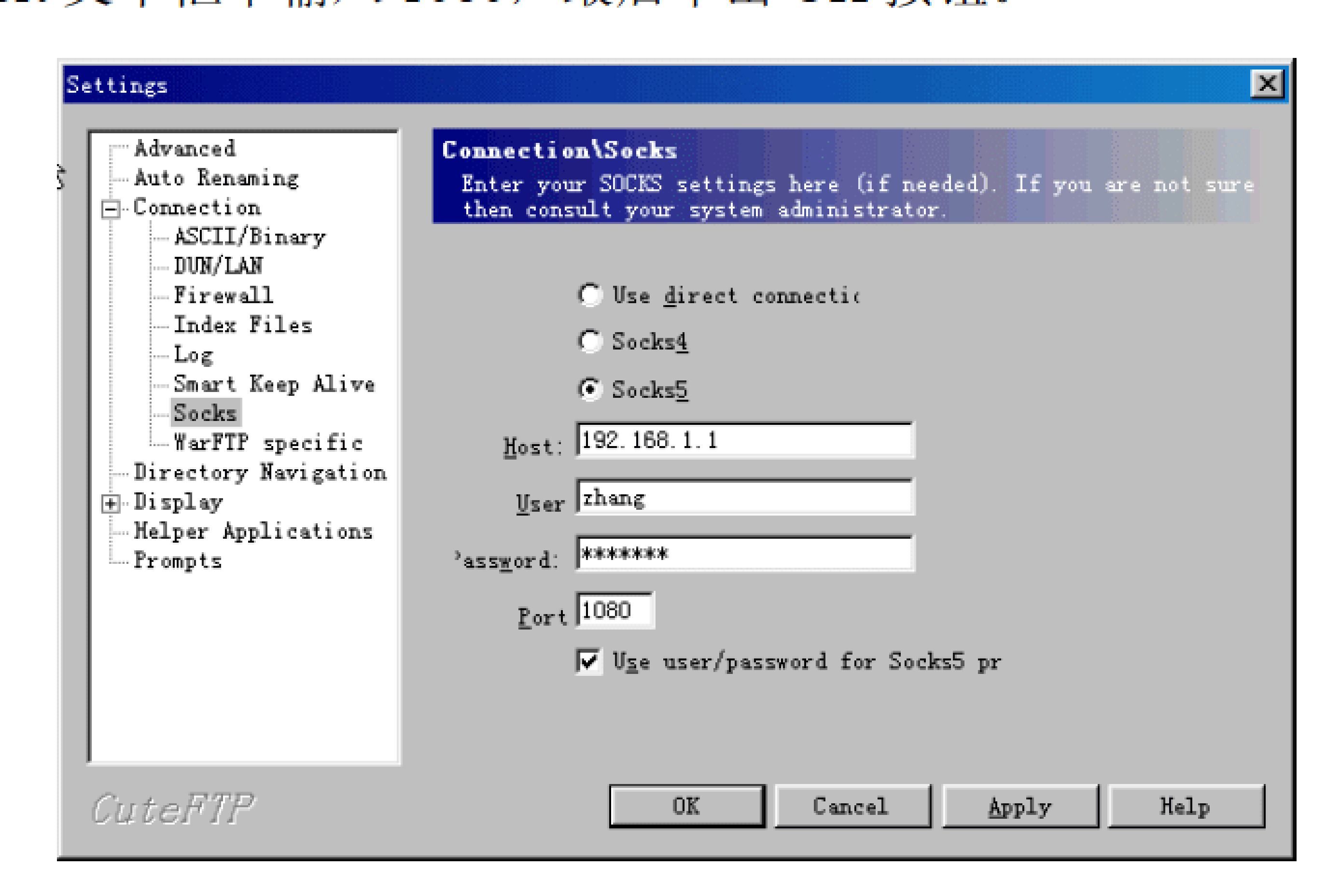


图 2-88 CuteFTP 浏览器代理服务器的设置

(4) 电子邮件客户端的设置(Outlook Express)

在 POP3 和 SMTP 的地址中都填写 WinGate 服务器的内部局域网 IP 地址，在帐号或用

户名中填入“帐号名#邮件服务器名”(注意用“#”号)。例如，在 www.tom.com 中申请了一个地址为 testuser@tom.com 的邮箱，那么帐号名中应填写“testuser#tom.com”，其他设置都一样，如图 2-89 所示。

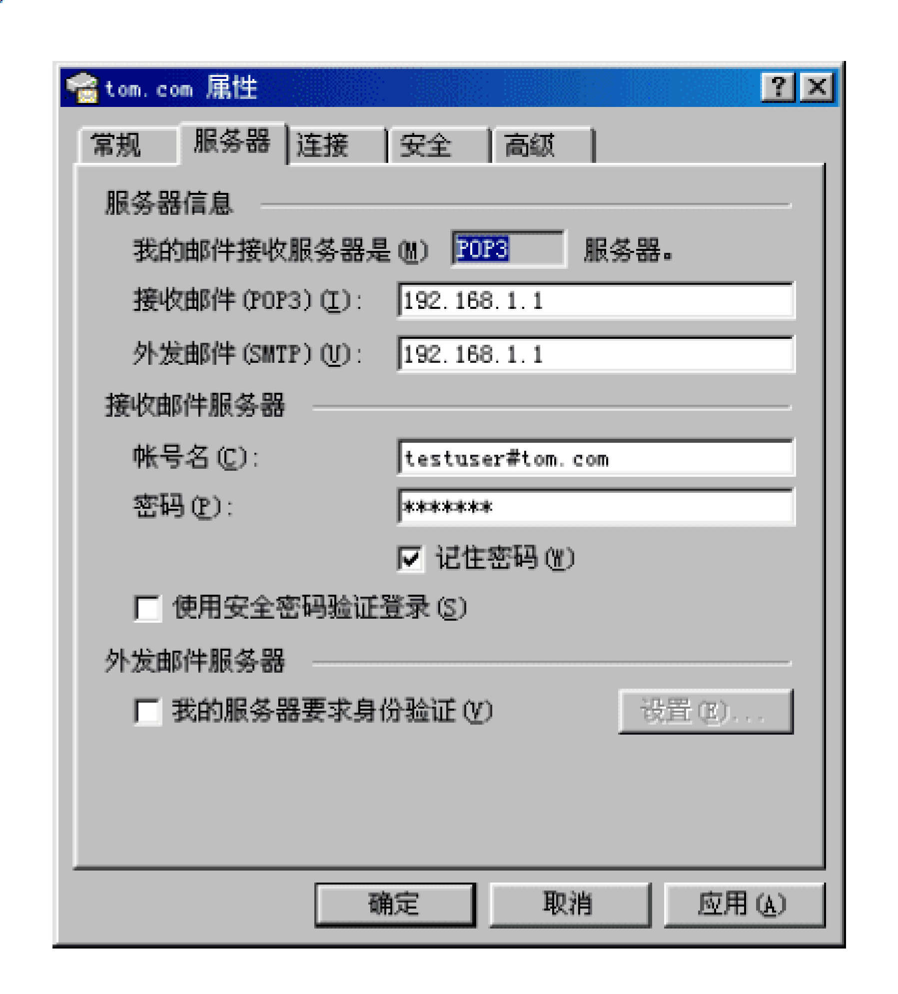


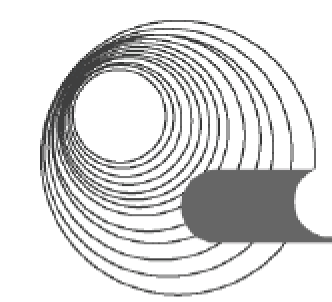
图 2-89　Outlook Express 代理服务器的设置

(5)　腾讯 QQ 2008

打开腾讯 QQ 2008 后，在用户登录对话框中，单击【网络设置】按钮，在【类型】中选择【SOCKS 5 代理】，在【地址】文本框中输入 WinGate 服务器的内部局域网 IP 地址，端口号为 1080。单击【测试】按钮，看代理服务器工作是否正常。如果正常，即可按正常程序输入 QQ 号码和密码就可使用了，如图 2-90 所示。



图 2-90　QQ 2008 代理服务器的设置



(6) NetAnts

打开 NetAnts 后，选择【选项】|【参数设置】|【代理】命令，在出现的【代理】对话框中输入以下内容：名称可任意填写，如填入 general，类型选择 SOCKS 5，地址输入 WinGate 服务器的内部局域网 IP 地址 192.168.1.1，端口号为 1080，如图 2-91 所示。

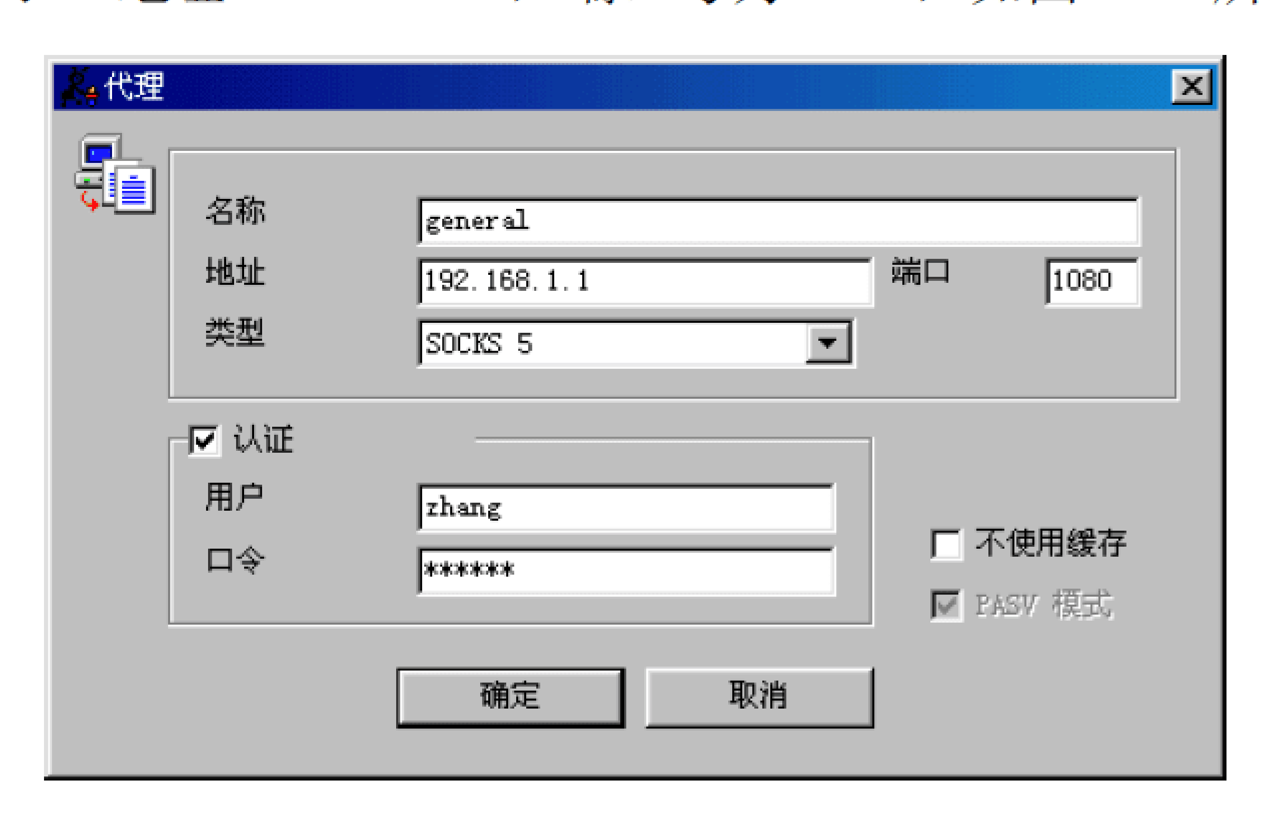


图 2-91　NetAnts 代理服务器的设置

(7) telnet

选择【开始】|【运行】命令，在打开的【运行】对话框中输入“telnet <WinGate 服务器的内部局域网 IP 地址>”，然后会出现列选框，再输入所要 telnet 的地址或域名即可。

(8) RealPlayer

安装好 RealPlayer 后，选择【开始】|【控制面板】| RealPlayer 命令，在打开的【首选项】对话框中切换到【代理服务器】选项卡，然后选中【手工配置 HTTP 代理服务器】单选按钮，并在【代理服务器】文本框中输入 WinGate 服务器的内部局域网 IP 地址，【端口】文本框中输入 80，如图 2-92 所示。

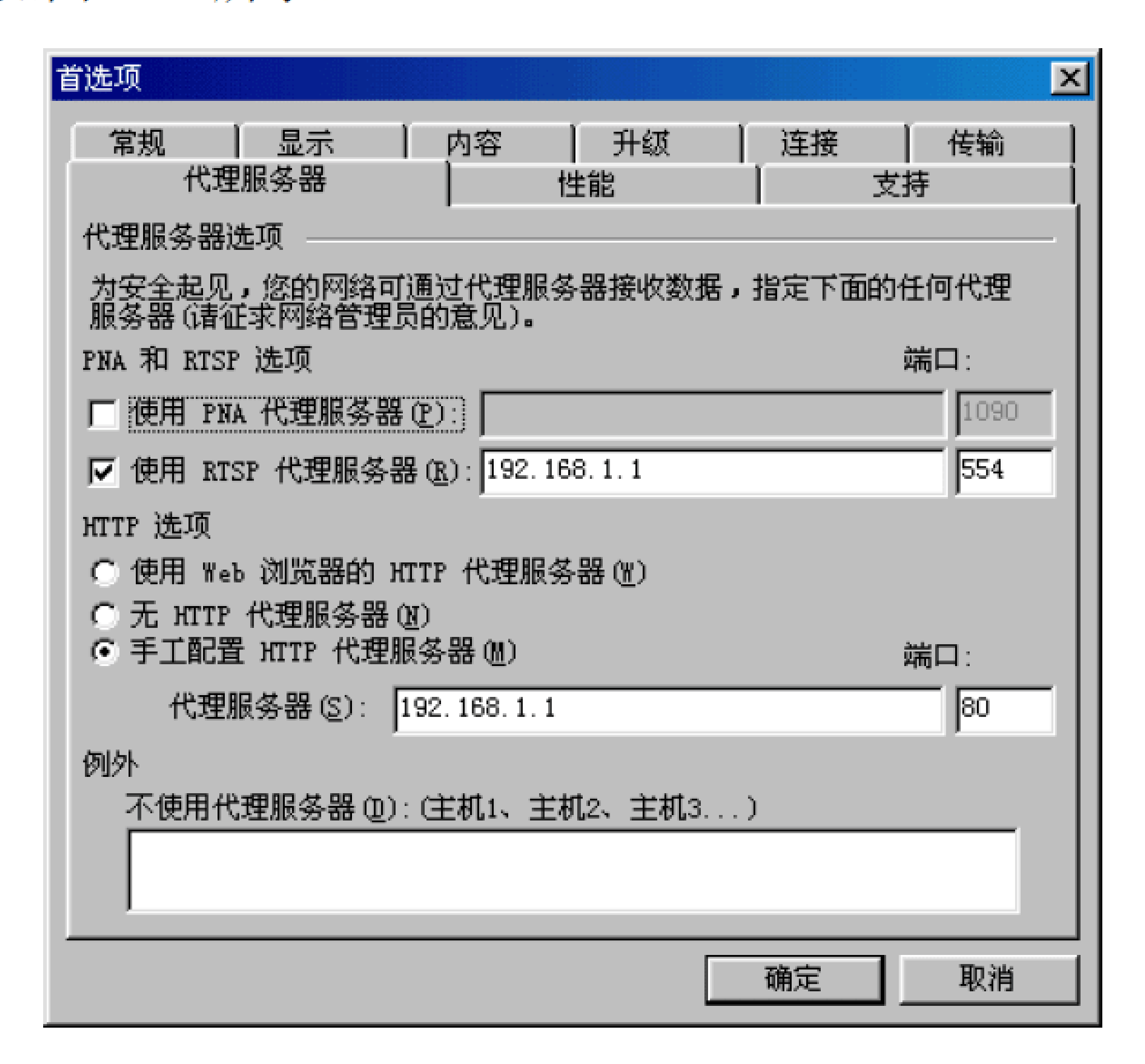


图 2-92　RealPlayer 代理服务器设置

2.6.1.3　Linux 下 Squid 代理服务器的配置与管理

Linux 环境下的代理服务器的软件较多，但实践证明被广泛应用的高性能代理服务器只有少数几个，Squid 就是其中之一。

对于 Web 用户来说，Squid 是一个高性能的代理缓存服务器，它支持 HTTP、FTP 和 GOPHER 协议。与一般代理缓存软件不同，Squid 用一个单独的、非模块化的、I/O 驱动的进程来处理所有客户端的请求。

Squid 将数据源缓存在内存中，同时也缓存 DNS 的查询结果。除此之外，它还支持非模块化 DNS 查询，对失败的请求进行消极缓存。Squid 支持 SSL 协议，支持访问控制。由于使用了 ICP(轻量级 Internet 缓存协议)，Squid 能够实现层叠的代理阵列，从而可最大限度地节省带宽。

Squid 由一个主要服务程序 Squid、一个 DNS 查询程序 dnsserver、几个重写请求和执行认证的程序，以及几个管理工具组成。当 Squid 启动后，它可派生出预先指定数目的 dnsserver 进程，而每一个 dnsserver 进程都可单独进行 DNS 查询，从而大大减少了服务器等待 DNS 查询的时间。

Squid 的代理方式既可以是传统代理，也可以是透明代理。由于透明代理比较复杂，这里只介绍传统代理的运行方式。在传统代理方式中，客户端不需要安装客户端软件，但需要对应用软件作相应的设置。如在 IE 中，需要设置代理服务器的地址和代理端口号。

1. Squid 代理服务器的安装

在 Red Hat Linux 的安装盘中都带有 Squid 代理服务器软件，也可以从网上下载安装包。执行如下命令即可完成安装：

```
#rpm -ivh squid-2.3-STABLE4-1.i386.rpm     //2.3-STABLE4-1 为 Squid 版本号
```

2. Squid 代理服务器的配置

Squid 有一个主要配置文件/etc/squid/squid.conf，该配置文件很长，默认的/etc/squid/squid.conf 长达到 2177 行之多。虽然 Squid 的配置文件很庞大，但是，若用户只是一个中小型网络提供代理服务，并且只使用一台代理服务器，那么只需要修改配置文件中的几个选项即可。下面列举了配置文件中需要修改的内容，并作简要介绍。

```
http_port 8080
cache_mem 32 MB
cache_dir /home/squid/cache 1200 16 256
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers 210.12.114.130
acl all src 0.0.0.0/0.0.0.0
http_access allow all
cache_mgr jim@abc.com.cn
```

(1) http_port

该选项用于定义 Squid 监听 HTTP 客户连接请求的端口。默认值是 3128，如果使用 HTTPD 加速模式则为 80。可以指定多个端口，但是所有指定的端口都必须在一条命令行上。

例如：

```
http_port 8080            表示代理服务器监听的端口为 8080
```

(2) cache_mem

该选项用于指定 Squid 可以使用的内存的理想值，单位为 B。

(3) cache_dir

该选项用于指定 Squid 用来存储对象的交换空间的大小及其目录结构。

```
cache_dir  <目录>  <大小>  <一级目录数> <二级目录数>
```

可以用多个 cache_dir 命令来定义多个这样的交换空间，并且这些交换空间可以分布不同的磁盘分区。“目录”(Directory)指明了该交换空间的顶级目录。“大小”定义了可用的空间总量，其单位是 MB。需要注意的是，Squid 进程必须拥有对该目录的读写权力。“Level-1”是可以在该顶级目录下建立的第一级子目录的数目，默认值为 16。同理，“Level-2”是可以建立的第二级子目录的数目，默认值为 256。为什么要定义这么多子目录呢？这是因为，如果子目录太少，则存储在一个子目录下的文件数目将大大增加，这样会导致系统寻找某一个文件的时间大大增加，从而使系统的整体性能急剧降低。所以，为了减少每个目录下的文件数量，我们必须增加所使用的目录的数量。如果仅仅使用一级子目录，则顶级目录下的子目录数目太大了，所以我们使用两级子目录结构。

那么，怎么来确定你的系统所需要的子目录数目呢？可以用下面的公式来估算。

已知量：

DS = 可用交换空间总量(单位 KB)/交换空间数目

OS = 平均每个对象的大小= 20KB

NO = 平均每个二级子目录所存储的对象数目= 256KB 单位

未知量：

L1 = 一级子目录的数量

L2 = 二级子目录的数量

计算公式：

$L1 \times L2 = DS/OS/NO$

注意这是个不定方程，可以有多个解。

如果不想 Squid 缓存任何文件，如某些存储空间有限的专有系统，可以使用 null 文件系统(这样就不需要那些缓存策略)：

```
cache_dir null /tmp
```

(4) cache_access_log

说明：指定客户请求记录日志的完整路径(包括文件的名称及所在的目录)，该请求可以是来自一般用户的 Http 请求或来自邻居的 ICP 请求。默认值为：

```
cache_access_log /var/log/squid/access.log
```

如果你不需要该日志，可以用以下语句取消：

```
cache_access_log none
```

(5)　cache_log

说明：指定 Squid 一般信息日志的完整路径(包括文件的名称及所在的目录)。默认路径为：

```
cache_log /var/log/squid/cache.log
```

(6)　dns_nameservers

该选项用来定义 Squid 进行域名解析时使用的域名服务器。因为在使用代理协议时，客户端并不进行域名查询，而是通过代理进行的，因此需要为代理服务器指定域名服务器来进行域名解析。例如：

```
dns_nameservers 210.12.114.130
```

(7)　acl

说明：定义访问控制列表。定义语法为：

```
acl aclname acltype string1 ...
acl aclname acltype "file" ...
```

当使用文件时，该文件的格式为每行包含一个条目。

acl type 可以是 src、dst、srcdomain、dstdomain、url_pattern、urlpath_pattern、time、port、proto、method、browser、user 中的一种。

分别说明如下：

- src 指明源地址。可用以下的方法指定：

```
acl aclname src ip-address/netmask ... (客户 IP 地址)
acl aclname src addr1-addr2/netmask ... (地址范围)
```

- dst 指明目标地址。语法为：

```
acl aclname dst ip-address/netmask ...(客户请求的服务器的 IP 地址)
```

- srcdomain 指明客户所属的域。语法为：

```
acl aclname srcdomain foo.com ... squid(将根据客户 IP 反向查询 DNS)
```

- dstdomain 指明请求服务器所属的域。语法为：

```
acl aclname dstdomain foo.com ...(由客户请求的 URL 决定)
```

注意，如果用户使用服务器 IP 而非完整的域名时，Squid 将进行反向的 DNS 解析来确定其完整域名，如果失败就记录为 none。

- time 指明访问时间。语法如下：

```
acl aclname time [day-abbrevs] [h1:m1-h2:m2]
```

day-abbrevs：S – Sunday、M – Monday、T – Tuesday、W – Wednesday、T – Thursday、F – Friday、S – Saturday。h1:m1 必须小于 h2:m2，表达式为[hh:mm-hh:mm]。

- port 指定访问端口。可以指定多个端口，比如：

```
acl aclname port 80 70 21 ...
acl aclname port 0-1024 ... (指定一个端口范围)
```

- proto 指定使用协议。可以指定多个协议：

```
acl aclname proto HTTP FTP ...
```

- method 指定请求方法。比如：

```
acl aclname method GET POST ...
```

这里定义了一个名为 all 的组，包括所有的主机。

(8) http_access

说明：根据访问控制列表允许或禁止某一类用户访问。如果某个访问没有相符合的项目，则默认为应用最后一条项目的“非”。比如最后一条为允许，则默认就是禁止。所以，通常应该把最后的条目设为 deny all 或 allow all 来避免安全性隐患。

(9) cache_mgr

说明：服务器管理者的电子邮件，当发生错误时，该地址会显示在错误页面上，便于用户联系。

3. 测试及管理方法

1) 重新启动 Squid 服务

当修改完配置文件后，需要重新启动才能使得 Squid 配置生效。其命令是：

```
#/etc/rc.d/init.d/squid restart
```

2) 初始化 Squid Cache 目录

在为 Squid 初始化 Cache 目录之前，先要更改这个目录的权限，其命令如下：

```
#chmod 0777 /home/squid/cache
#squid -z
```

3) 测试

在客户端的 IE 浏览器中需要设置代理服务器的 IP 地址和端口号，端口号由 http_port 选项指定。

2.6.2 典型例题分析

例 1 阅读以下说明，回答问题 1～问题 3，将解答填入答题纸对应的解答栏内。(2008 年 5 月下午试题一)

【说明】

某内部局域网连接方式如图 2-93 所示，客户机通过代理服务器访问 Internet。代理服务器的公网 IP 为 61.194.101.35/24。

在主机 host1 的 Windows 命令行窗口输入 tracert www.abc.com 命令后，测试到目的站点所经过的连接情况，如图 2-94 所示。

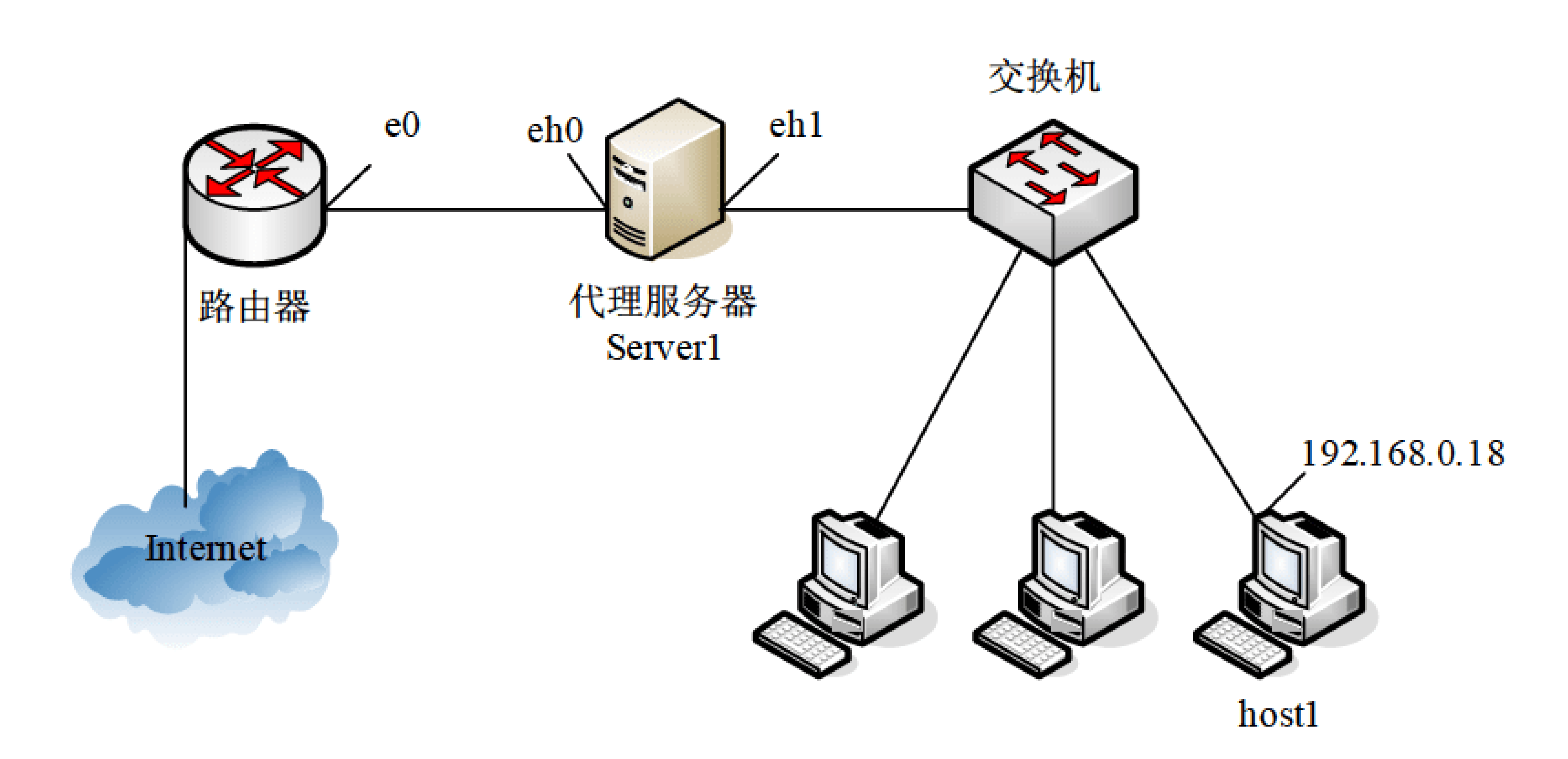


图 2-93　某内部局域网连接方式

```
C:\Documents and Settimgs\User>tracart    www.abc.com
Tracing route to www.abc.com [210.200.3.143]
Over a maximum of 30 hops:
    1    <1ms     <1ms     <1ms     192.168.1.1
    2    1580ms   63ms     11ms     61.194.101.254
    3    4ms      1ms      1ms      202.200.29.141
    4    1ms      1ms      1ms      202.200.29.9
    5    <1ms     <1ms     <1ms
```

图 2-94　测试结果

【问题 1】(2 分)

下列选项中___(1)___是 Windows 中代理服务器软件。

A. WinGate　　B. outlook　　C. IIS　　D. winzip

【问题 2】(8 分)

参照图 2-93 和图 2-94，为 Server1 网卡 eth1 配置 Internet 协议属性参数。

IP 地址：　　___(2)___ (2 分)

子网掩码：　　___(3)___ (2 分)

(3) 备选答案：

A. 255.255.255.0　　B. 255.255.254.0　　C. 255.255.255.128

为 Server1 网卡 eth0 配置 Internet 协议属性参数。

IP 地址：　　___(4)___ (1 分)

子网掩码：　　___(5)___ (1 分)

默认网关：　　___(6)___ (2 分)

【问题 3】(5 分)

参照图 2-93 和图 2-94，为 host1 配置 Internet 协议属性参数。

IP 地址：　　___(7)___ (1 分)

子网掩码：　　___(8)___ (2 分)

默认网关： (9) (2 分)

分析：

【问题 1】

代理服务器软件运行于局域网上的一台计算机上，称其为代理服务器或网关。代理服务器将网络分成了两段：一段连接 Internet，另一段连接局域网。局域网内的每台计算机都可以通过代理服务器访问 Internet，它们共享代理服务器的一个 IP 地址和同一帐号。通常代理服务器的实现有 Internet 连接共享(Internet Connection Share，ICS)、WinGate 以及 SyGate 等多种方式。

【问题 2】

tracert 命令通过发送包含不同 TTL 的 ICMP 报文并监听回应报文，来探测到达目的计算机的路径。路径将以列表形式显示，显示了从本机到目的主机所经过的跳数、各跳节点的 IP 地址及经过每跳节点所需要的时间。

代理服务器 Server1 的 eth1 接口是内部主机的网关。输入 tracert www.abc.com 命令后，由测试到目的站点所经过的连接情况可知，内部网络的网关地址为 192.168.1.1。内部主机 host1 的 IP 地址为 192.168.0.18，网关和内部主机应处于同一网段，由“最长前缀匹配”原则可知，子网掩码为 255.255.254.0。

代理服务器 Server1 的公网 IP 为 61.194.101.35/24，可知 IP 地址为 61.194.101.35，子网掩码为 255.255.255.0。eth0 接口的默认网关为与其直接相连的路由器地址，从连接情况图可知为 61.194.101.254。

【问题 3】

由内部局域网连接方式可知，主机 host1 的 IP 地址为 192.168.0.18，根据【问题 2】的分析可知，子网掩码与代理服务器 Server1 的 eth1 相同，为 255.255.254.0。默认网关为内部网络的网关 IP 地址，由【问题 2】的分析可知为 192.168.1.1。

答案：

【问题 1】

(1) A

【问题 2】

(2) 192.168.1.1　　(3) B

(4) 61.194.101.35　　(5) 255.255.255.0

(6) 61.194.101.254

【问题 3】

(7) 192.168.0.18　　(8) 255.255.254.0

(9) 192.168.1.1

例 2 阅读下列说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题二)

【说明】

某局域网结构如图 2-95 所示。服务器安装 Windows Server 2003 并配置 NAT 服务，客户机可以通过 NAT 服务器访问 Internet。

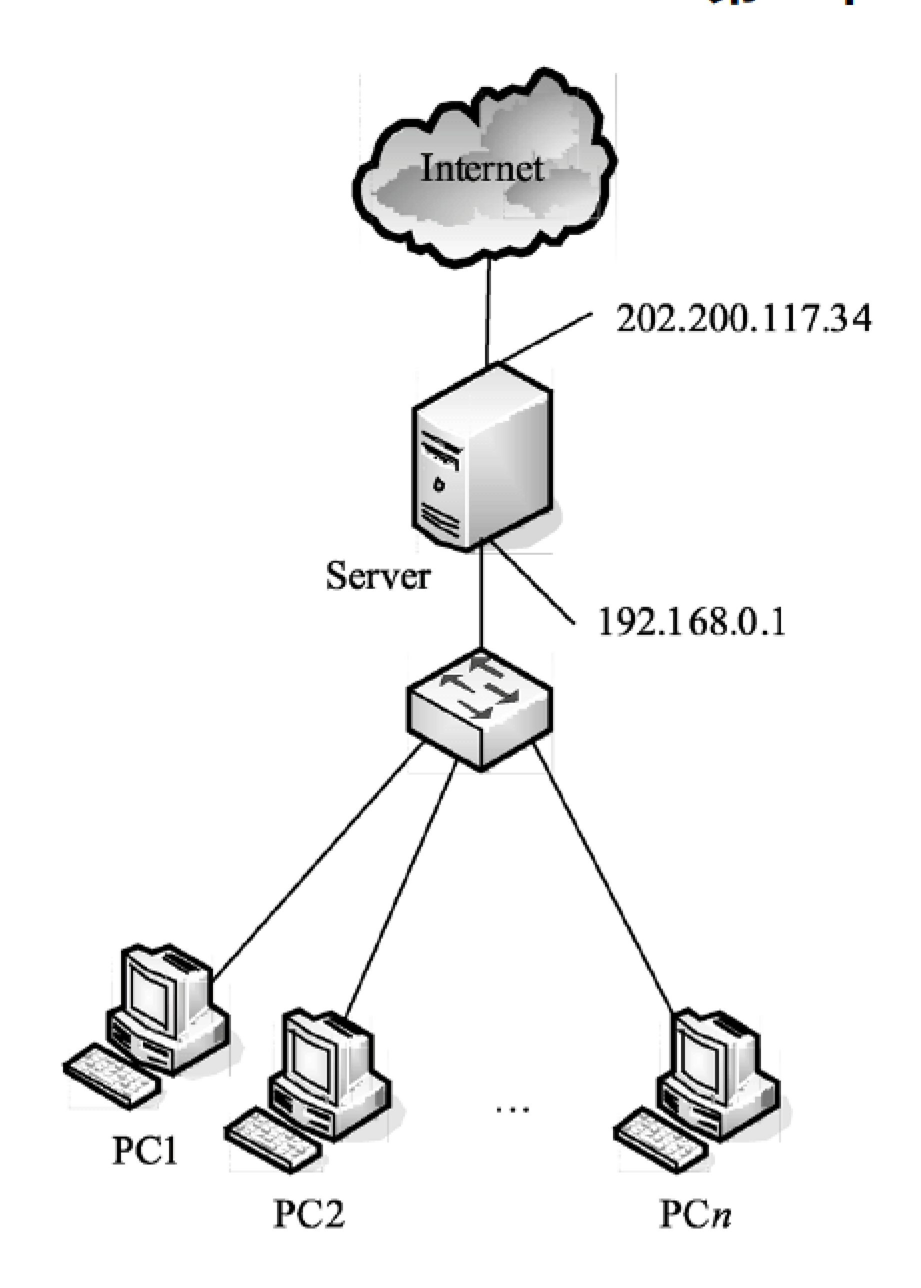


图 2-95　某局域网连接示意

【问题 1】(2 分)

Windows Server 2003 新增的功能有：__(1)__。

A．MSN Messager

B．流媒体服务(Windows Media Services，WMS)

C．活动目录(Active Directory)

D．Internet 信息服务

【问题 2】(4 分)

在 Server 上进行 NAT 服务器配置时，若“接口 2”的配置如图 2-96 所示，则其 IP 地址应设置为__(2)__。“NAT/基本防火墙”属性如图 2-97 所示，单击【排除】按钮，在弹出的对话框中，输入的 IP 地址应为__(3)__。

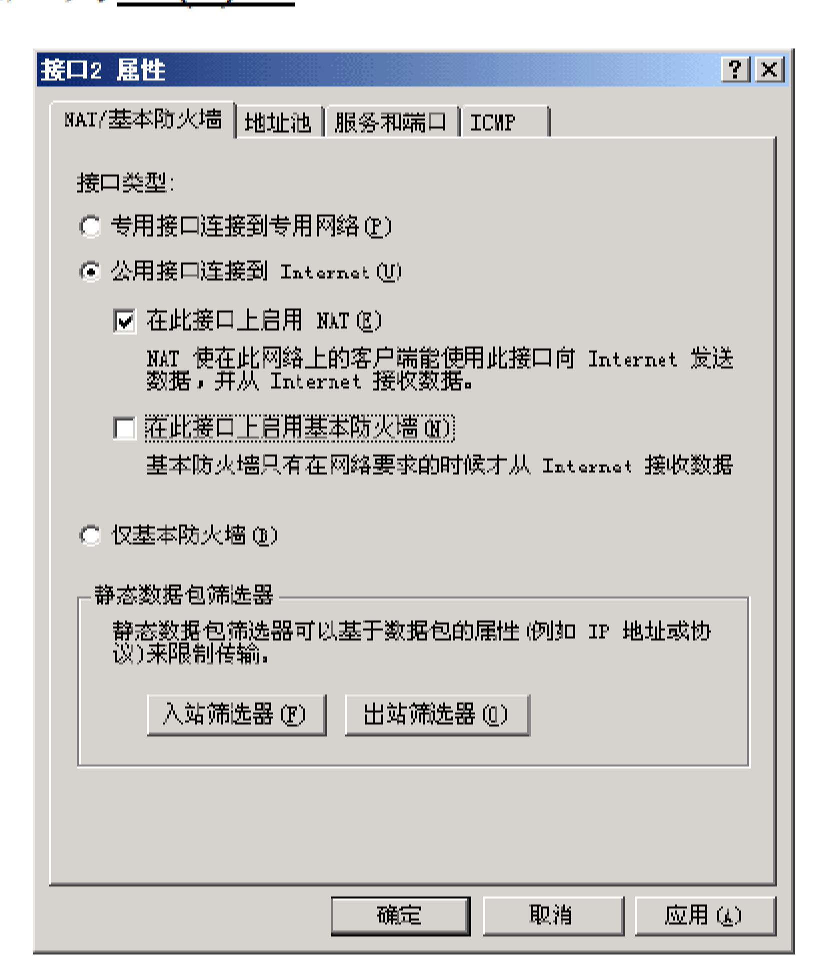


图 2-96　【接口 2 属性】对话框

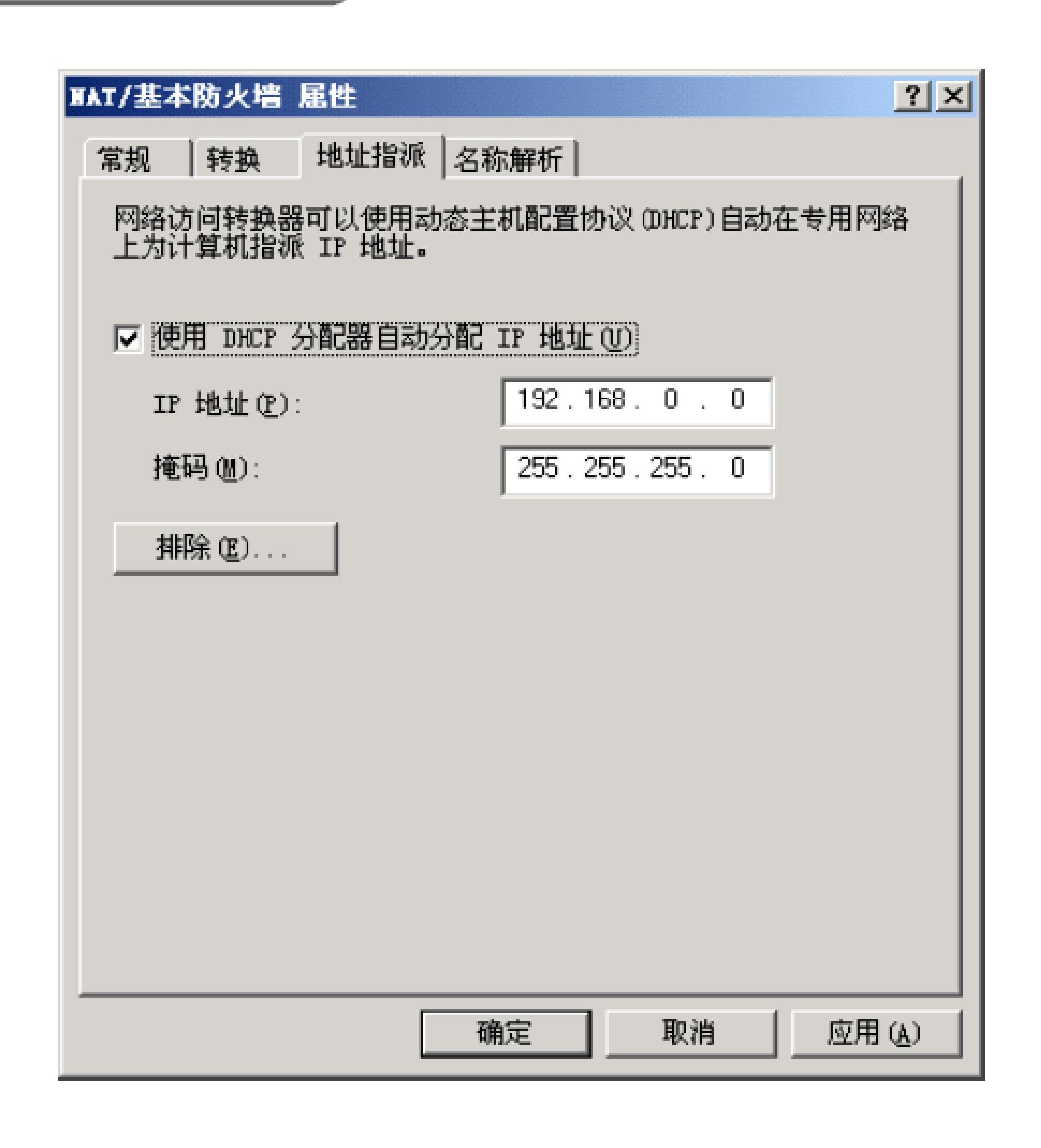


图 2-97 【地址指派】选项卡

【问题 3】(3 分)

完成 Server 的安装、配置后，在如图 2-98 所示的客户机【Internet 协议(TCP/IP)属性】对话框中，IP 地址的配置方法是__(4)__；网关地址为__(5)__。

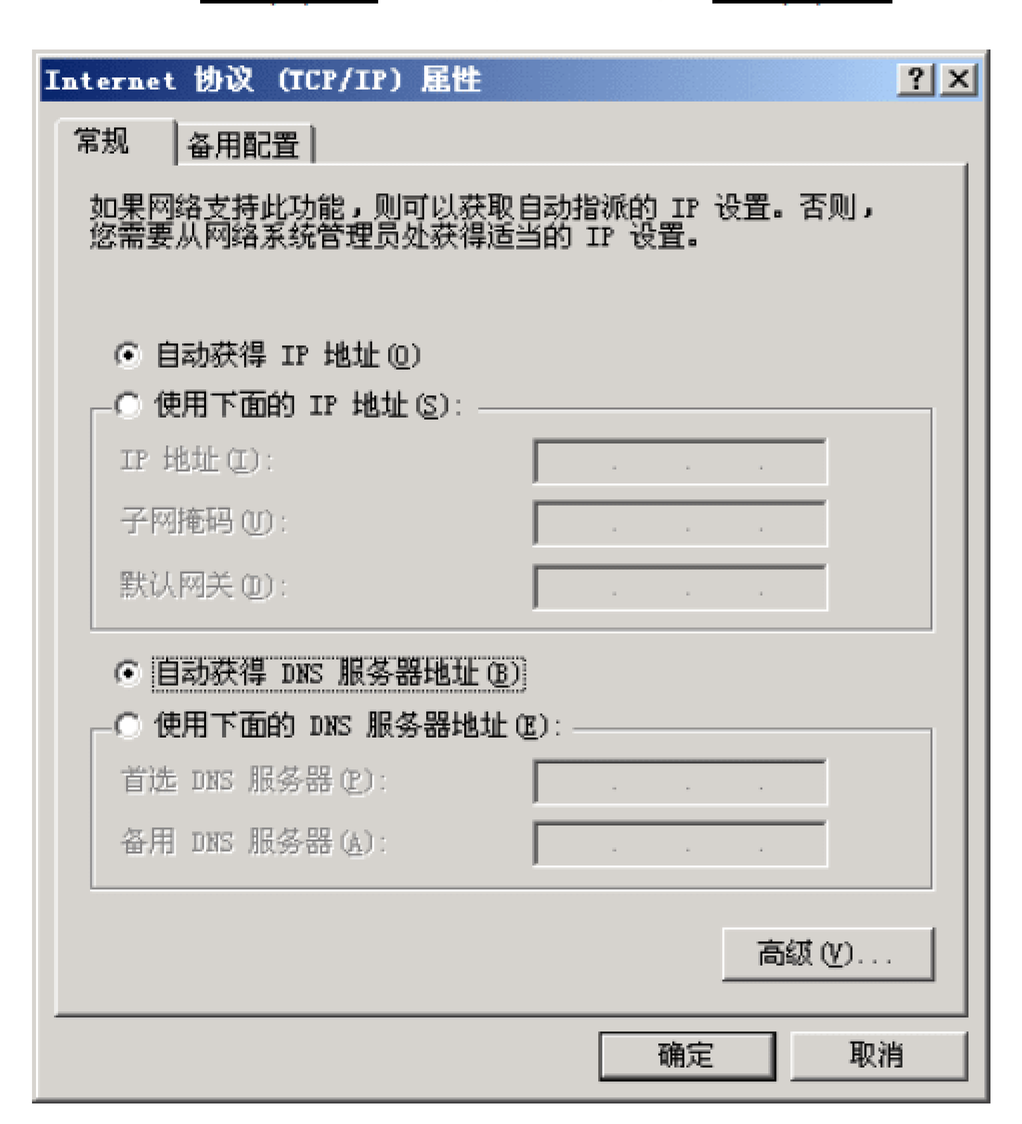


图 2-98 【常规】选项卡

【问题 4】(3 分)

在客户机 PC1 上启动 IE 访问 Web 站点时，若系统提示“因站点内容被 IE 增强的安全配置堵塞而不能正常显示页面”，在 IE 中依次切换到【工具】、【Internet 选项】、【安全】选项卡，在“指定安全设置”选项区中选中 Internet 选项(如图 2-99 所示)，通过配置解决上述问题的方法是__(6)__。



图 2-99　【Internet 选项】对话框

【问题 5】(3 分)

在 Windows Server 2003 中，通过__(7)__配置 DHCP 服务器；本题中 DHCP 服务器的 IP 地址为__(8)__。

(7) A．IIS6.0　　B．服务器角色　　C．Active Directory　　D．代理服务器

分析：

【问题 1】

Windows Server 2003 在 Windows 2000 Server 的基础上增加了许多新功能，包括配置流程向导、远程桌面连接(TS)、Internet 信息服务(IIS6.0)、简单的邮件服务器(POP3)、WMS 流式媒体服务器等。

【问题 2】

作为 NAT 路由器的那台服务器必须配置两个网卡。其中一个网卡连接到互联网。这个网卡必须指定一个由你的互联网服务提供商向你提供的 IP 地址(即 202.200.117.34)。另一个网卡连接到你的专用网络。在你的专用网上不需要合法的 IP 地址。你可以随机选择 IP 地址段，本题选择了一个私有地址(即 192.168.0.1)。从属性图中可以看出，接口 2 为连接公网的接口，因此其 IP 地址应设置为公网合法 IP 地址 202.200.117.34。

NAT 服务器同时具有 DHCP 分配服务的功能，为内网用户提供 DHCP 服务，其 IP 地址为内网接口的地址，即 192.168.0.1，DHCP 地址池的 IP 地址范围应与内网接口处于同一网段，即范围是 192.168.0.1～192.169.0.254，故需将服务器的地址 192.168.0.1 从 DHCP 地址池中排除。

【问题 3】

因为 NAT 服务器具有 DHCP 服务的功能，客户端可通过 DHCP 服务器自动获得 IP 地址、子网掩码、网关、DNS 等信息。

客户机应与服务器的内网接口的地址处于同一网段内，客户机的网关应为服务器内网接口的 IP 地址，即 192.168.0.1。

【问题 4】

在客户机 PC1 上启动 IE 访问 Web 站点时，若系统提示“因站点内容被 IE 增强的安全配置堵塞而不能正常显示页面”，原因是 IE 浏览器安全级别设置为高。在 IE 中依次切换到【工具】、【Internet 选项】、【安全】选项卡，在“指定安全设置”选项区中选中 Internet 将【安全级】设置为【中】或以下级别；或单击【自定义级别】按钮，将【安全级】设置为【中】或以下级别。

【问题 5】

Windows Server 2003 的管理工具中有一项功能叫做“管理您的服务器”，启动该工具之后，可以看到当前服务器上启用的所有服务，并可对这些服务进行管理。单击该界面上的【添加或删除角色】链接，将启动一个配置服务器的向导。单击【下一步】按钮进入【服务器角色】界面，在 Windows Server 2003 支持的角色列表中选择 DHCP 服务器并单击【下一步】按钮，开始启用和配置文件服务的过程。因此在 Windows Server 2003 中，通过服务器角色配置 DHCP 服务器。

NAT 服务器同时具有 DHCP 服务器的功能，为内网用户提供 DHCP 服务，其 DHCP 服务器的 IP 地址即为 NAT 服务器内部网络接口的 IP 地址，即 192.168.0.1。

答案：

【问题 1】

(1) B

【问题 2】

(2) 202.200.117.34

(3) 192.168.0.1

【问题 3】

(4) 选中【自动获得 IP 地址】单选按钮

(5) 192.168.0.1

【问题 4】

(6) 将【安全级】设置为【中】或以下级别；或单击【自定义级别】按钮，将【安全级】设置为【中】或以下级别。

【问题 5】

(7) B

(8) 192.168.0.1

2.6.3 同步练习

1．阅读以下说明，回答问题 1～问题 5，将答案填入对应的答案栏内。

【说明】

某小型公司已经建成了一个局域网，内部计算机的 IP 地址为 192.168.1.2～192.168.1.254，子网掩码为 255.255.255.0，DNS 和默认网关都没有设置。该公司在 ISP 处申请了 Internet 接入，接入方式是以太网，ISP 分配给了一个固定的 IP 地址为 222.152.199.33、

子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68。该公司使用一台 PC 服务器作为代理服务器以实现整个公司上网，代理软件准备采用 WinGate 5.0，代理方式采用透明代理，网络拓扑结构如图 2-100 所示。

【问题 1】(1)处该填写什么内容？

【问题 2】(2)处该填写什么内容？

【问题 3】(3)处该填写什么内容？

【问题 4】(4)处该填写什么内容？

【问题 5】需要安装何种软件并作何种设置？若客户机使用 IE 浏览网页，该如何设置 IE。

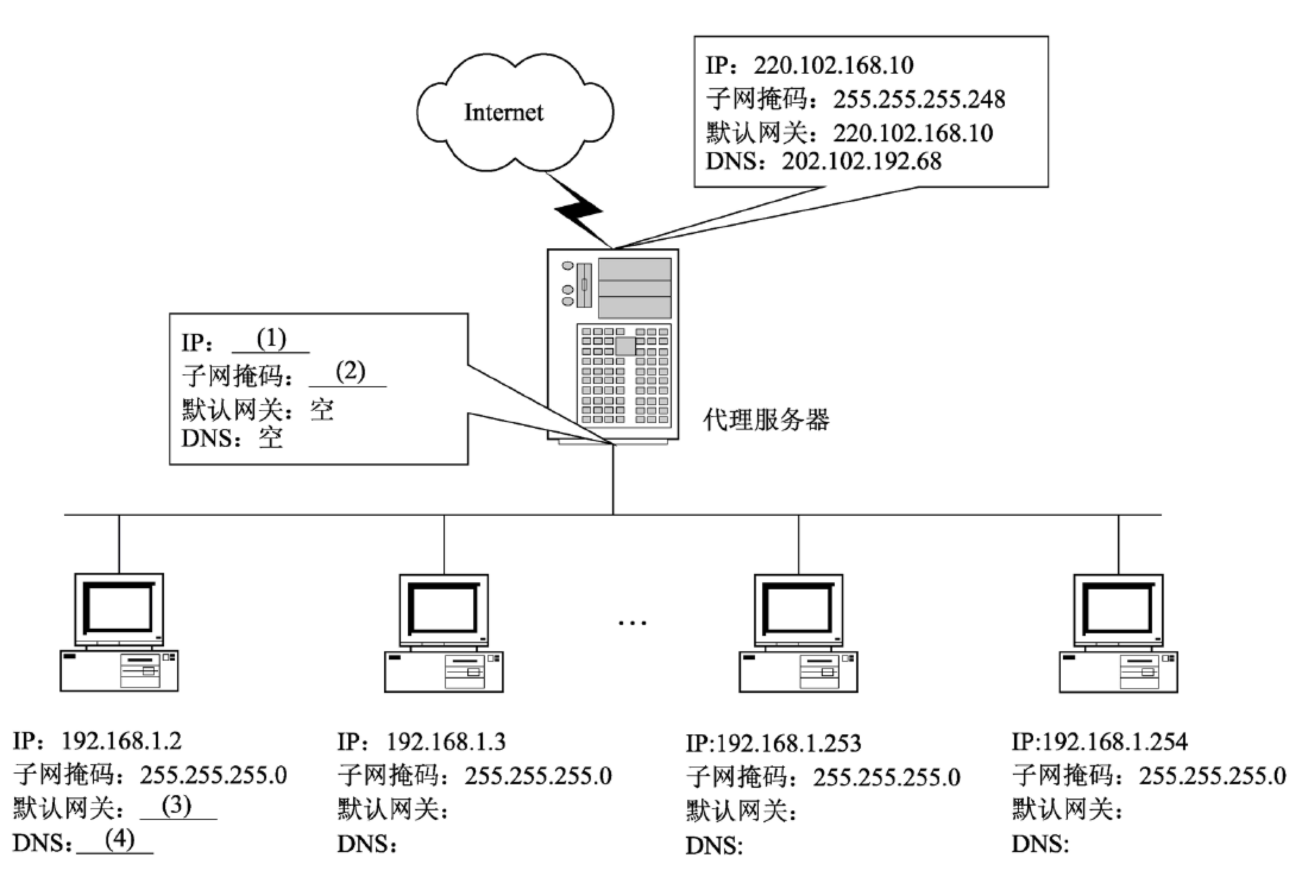


图 2-100　同步练习 1 拓扑结构

2．阅读以下说明，回答问题 1～问题 6，将答案填入对应的答案栏内。

【说明】

在 Linux 下安装配置代理服务 Squid，Squid 服务程序/usr/sbin/squid 需要读取配置文件/etc/squid/squid.conf，以下是该文件内容的一个片段。

```
http_port 4444
cache_mem 32 MB
cache_dir  /home/squid/cache 1024 16 256
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers 210.45.12.31
acl denyip dst 61.136.135.04/255.255.255.255
acl all scr 0.0.0.0/0.0.0.0
```

```
http_access deny denyip
http_access allow all
cache_mgr root@weboa.com.cn
```

【问题 1】客户机的 IE 的代理服务器端口号应设置为多少?

【问题 2】该代理服务器缓冲区放在哪里?大小是多少?能建多少一级目录，多少二级目录?

【问题 3】该代理服务器使用的域名服务器 IP 地址是什么?

【问题 4】文件中阴影的两行的作用是什么?

【问题 5】#squid –z 命令的作用是什么?

【问题 6】修改完配置文件后，如何使其立即生效?(不重新启动计算机)

2.6.4 同步练习参考答案

1.

【问题 1】192.168.1.1

【问题 2】255.255.255.0

【问题 3】192.168.1.1

【问题 4】202.102.192.68

【问题 5】需要安装 WinGate 客户端，IE 不需做任何设置。

2.

【问题 1】4444

【问题 2】/home/squid/cache 1024 16 256

【问题 3】210.45.12.31

【问题 4】禁止所有的客户机访问 IP 地址为 61.136.135.04 的站点。

【问题 5】为 Squid 初始化 Cache 目录。

【问题 6】#/etc/rc.d/init.d/squid restart

2.7 DHCP 服务器配置

2.7.1 考点辅导

2.7.1.1 DHCP 基础

1. DHCP 是什么?

动态主机分配协议(DHCP)是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作(如 DNS、WINS、Gateway 的设置)。

在使用 TCP/IP 协议的网络上，每一台计算机都拥有惟一的计算机名和 IP 地址。IP 地址(及其子网掩码)使用与鉴别它所连接的主机和子网，当用户将计算机从一个子网移动到另一个子网的时候，一定要改变该计算机的 IP 地址。如采用静态 IP 地址的分配方法将增加网络管理员的负担，而 DHCP 可以让用户将 DHCP 服务器中的 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机，从而减轻了网络管理员的负担。

在使用 DHCP 时，整个网络至少有一台服务器上安装了 DHCP 服务，其他要使用 DHCP 功能的工作站也必须设置成利用 DHCP 获得 IP 地址。如图 2-101 所示是一个支持 DHCP 的网络实例。DHCP 是基于客户机/服务器模型设计的，DHCP 客户机和 DHCP 服务器之间通过收发 DHCP 消息进行通信。

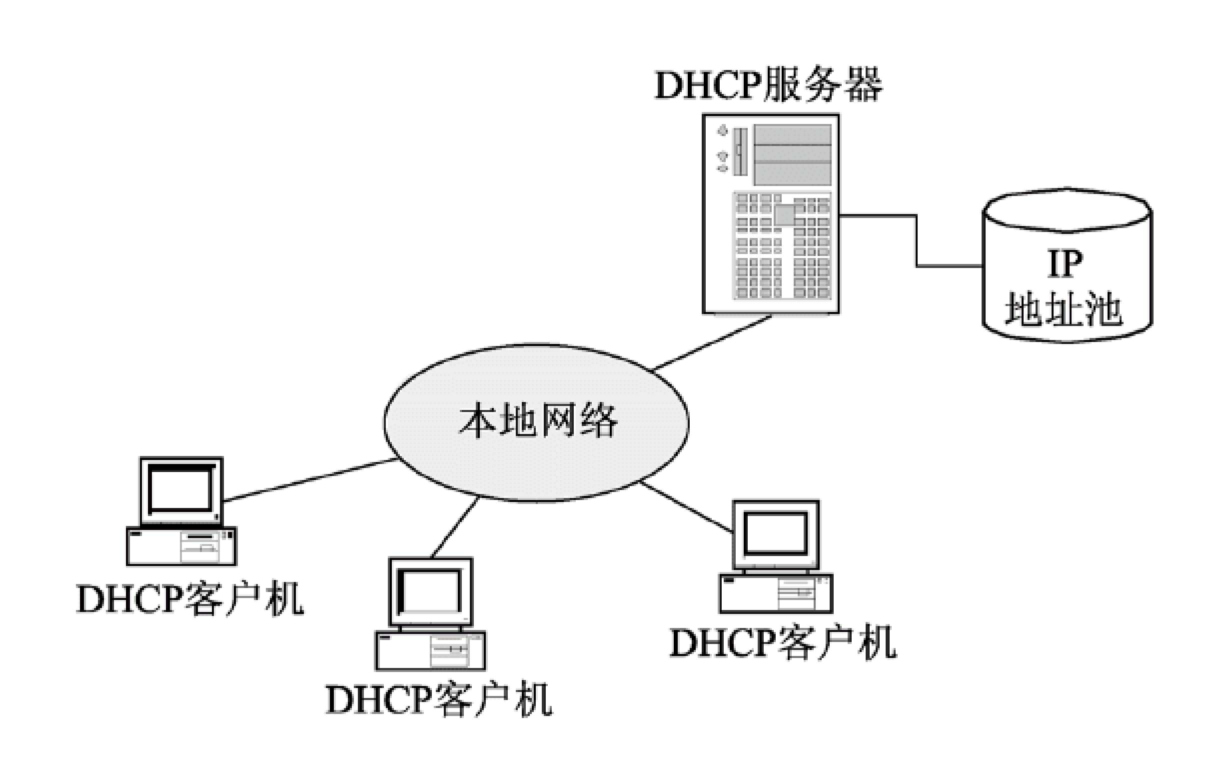


图 2-101　DHCP 服务工作原理

2. 使用 DHCP 的优点

1) 安全可靠

DHCP 可避免因手工设置 IP 地址等参数可能产生的错误，同时也可避免把一个 IP 地址分配给多台工作站所造成的地址冲突。

2) 网络配置自动化

使用 DHCP 服务器可大大缩短配置或重新配置网络中工作站所花费的时间。

3) IP 地址变更自动化

DHCP 地址租约的更新过程将有助于确定哪个客户的设置需要经常更新(如使用笔记本的客户经常更换地点)，且这些变更由客户机与 DHCP 服务器自动完成，无须网络管理员干涉。

3. 与 DHCP 相关的专业术语

(1) DHCP 客户：是指通过 DHCP 来获得网络配置参数的 Internet 主机。通常就是普通用户的工作站。

(2) DHCP 服务器：是提供网络设置参数给 DHCP 客户的 Internet 主机。

(3) DHCP/BOOTP 中继代理：是在 DHCP 客户和服务器之间转发 DHCP 消息的主机或路由器。

(4) 作用域：是一个网络中的所有可分配的 IP 地址的连续范围。它主要用来定义网络中单一的物理子网的 IP 地址范围。作用域是服务器用来管理分配给网络客户的 IP 地址的主要手段。

(5) 超级作用域：是一组作用域的集合。它用来实现同一个物理子网中包含多个逻辑 IP 子网。在超级作用域中只包含一个成员作用域或子作用域的列表。然而超级作用域并不用于设置具体的范围。子作用域的各种属性需要单独设置。

(6) 排除范围：是不分配的 IP 地址序列。它保证在这个序列中的 IP 地址不会被 DHCP 服务器分配给客户。

(7) 租约时间：是 DHCP 服务器指定的时间长度，在这个时间范围内客户机可以使用所获得的 IP 地址。当客户机获得 IP 地址时，租约被激活；在租约到期前，客户机需要更新 IP 地址的租约；当租约过期或从服务器上删除时，租约停止。

(8) 选项类型：选项类型是 DHCP 服务器给 DHCP 工作站分配服务租约时分配的其他客户配置参数。经常使用的选项包括默认网关的 IP 地址、WINS 服务器及 DNS 服务器。一般在设置每个范围时这些选项都被激活。

4. DHCP 服务器的工作原理

DHCP 客户使用两种不同的过程来与 DHCP 服务器通信并获得配置信息。DHCP 服务器是通过客户机租用网络地址来工作的，其租用过程的步骤随客户机是初始化还是续订其租约而不同。当客户计算机启动并尝试加入网络时，它将执行初始化过程。在客户机拥有租约之后将执行续订过程，但是需要使用服务器续订该租约。

1) 初始化租约过程

启用 DHCP 的客户机首次启动时，会自动执行初始化过程以便从 DHCP 服务器获得租约。下面介绍主要的几个过程，如图 2-102 所示。

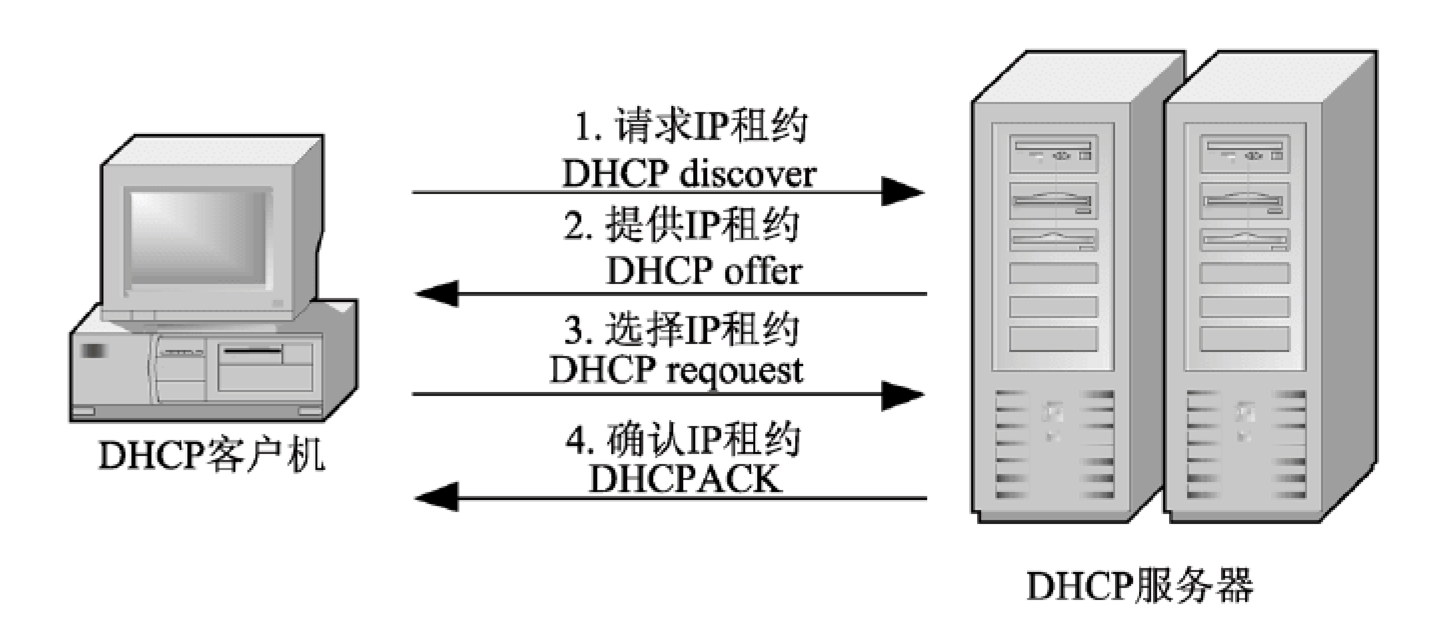


图 2-102 DHCP 初始化租约过程

(1) 请求 IP 租约：DHCP 客户机在本地子网中先发送 DHCP discover(DHCP 发现)消息，此消息以广播的形式发送，因为客户机还不知道 DHCP 服务器的 IP 地址。

(2) 提供 IP 租约：DHCP 服务器可通过包含为客户机租约提供的 IP 地址的 DHCP 提供(DHCPOFFER)；在 DHCP 服务器收到 DHCP 客户机广播的 DHCP discover 信息后，它向 DHCP 客户机发送 DHCP offer(DHCP 提供)消息进行响应，在消息中包括一个可租用的 IP 地址。

(3) 选择 IP 租约：一旦客户机收到 DHCP offer 信息，它会发送 DHCP request(DHCP 请求)信息到服务器，表示它将使用服务器所提供的 IP 地址。

(4) 确认 IP 租约：DHCP 服务器在收到 DHCP request 信息后，即发送 DHCP positive(DHCP 确认)确认信息，以确定此租约成立，而且此信息中还包含其他 DHCP 选项

信息。

客户机一旦接收到确认消息，就使用消息回复中的信息来配置其 TCP/IP 属性并加入网络。

在极少数情况下，DHCP 服务器可交替地向客户机返回 DHCP 否定确认消息。当客户机请求对于网络无效或重复的地址时可能会发生这种情况。如果客户机接收到否定确认消息，则当前的初始化过程失败。在这种情况下，客户机在第一步启动并重复如上所述的过程。

2)　租约续订过程

当 DHCP 客户机关闭并在相同的子网上重新启动时，它一般能获得和它关机之前的 IP 地址相同的租约。经过 50%的客户机租约时间后，客户机会尝试通过 DHCP 服务器来续订其租约。具体步骤如下。

(1)　客户机直接向它所租用的服务器发送 DHCP 请求消息(DHCPrequest)，以续订和扩展当前的地址租约。

(2)　如果可访问到服务器，它通常向客户机发送 DHCP 确认消息(DHCPack)，该客户机续订当前租约。同时，与初始租约过程中一样，其他 DHCP 选项信息也包含在该回复消息中。自客户机首先获得租约之后，只要有选项信息发生变化，客户机就会相应地更新其配置。

(3)　如果客户机不能与其最初的 DHCP 服务器通信，则客户机会一直等到它进入重新绑定状态。客户机在到达该状态时，会尝试通过任何可用的 DHCP 服务器来续订其当前租约。

(4)　如果服务器用 DHCP 提供消息(DHCP offer)进行响应以更新当前客户机租约，则客户机可根据提供服务器来续订其租约并继续运行。

(5)　如果租约过期并且未联系到服务器，则客户机必须立即中止使用其租用的 IP 地址。

(6)　客户机按照其初始启动操作期间使用的相同过程来获得新的 IP 地址租约。

5. DHCP 客户机的设置

DHCP 服务器安装、设置完成后，客户机就可开始启用 DHCP 功能。

1)　启用 Windows 95/98 客户机的 DHCP 功能

(1)　右击【网上邻居】图标，在弹出的快捷菜单中选择【属性】命令，在弹出的对话框中，单击 TCP/IP 选项，单击【属性】按钮。

(2)　选中【自动获得 IP 地址】单选按钮即可。

2)　启用 Windows 2000/XP/2003 客户机的 DHCP 功能

(1)　右击【网上邻居】图标，选择【属性】命令，在弹出的对话框中，右击【本地连接】图标，在出现的对话框中选中【Internet 协议(TCP/IP)】复选框，单击【属性】按钮。

(2)　选中【自动获得 IP 地址】单选按钮即可。

3)　查看、更新和释放 IP 地址租约

对于启用 DHCP 功能的 Windows 2000/XP 客户机，若要查看、更新和释放 IP 地址租约，可以使用 ipconfig 工具来完成。该诊断命令显示所有当前的 TCP/IP 网络配置值。该命令在运行 DHCP 系统上的特殊用途是，允许用户决定 DHCP 配置的 TCP/IP 配置值。

其命令格式是：

```
ipconfig [/all | /renew [adapter] | /release [adapter]]
```

各参数说明如下。

/all：产生完整显示。在没有该开关的情况下 ipconfig 只显示 IP 地址、子网掩码和每个网卡的默认网关值。

/renew [adapter]：更新 DHCP 配置参数。该选项只在运行 DHCP 客户端服务的系统上可用。要指定适配器名称，请输入使用不带参数的 ipconfig 命令显示的适配器名称。

/release [adapter]：发布当前的 DHCP 配置。该选项禁用本地系统上的 TCP/IP，且只 DHCP 客户端上可用。要指定适配器名称，请输入使用不带参数的 ipconfig 命令显示的适配器名称。

如果没有参数，那么 ipconfig 实用程序将向用户提供所有当前的 TCP/IP 配置值，包括 IP 地址和子网掩码。

对于启用 DHCP 的 Windows 95 和 Windows 98 客户机，请使用 winipcfg 命令的 all、release 和 renew 选项，而不是 ipconfig /all/release 和 ipconfig /renew 命令来查看、释放或更新客户的 IP 配置租约。

2.7.1.2　Windows Server 2003 下 DHCP 服务器的配置与管理

1. DHCP 服务器的安装

安装 DHCP 服务器的步骤如下。

(1) 选择【开始】|【设置】|【控制面板】命令，在打开的【控制面板】窗口中双击【添加或删除程序】图标，然后在出现的对话框中单击【添加/删除 Windows 组件】选项，打开如图 2-103 所示的对话框。



图 2-103 【Windows 组件向导】对话框

(2) 在【Windows 组件向导】对话框中，选中【网络服务】复选框，然后单击【详细信息】按钮，在出现的【网络服务】对话框中，选中【动态主机配置协议(DHCP)】复选框。

单击【确定】按钮，如图 2-104 所示。

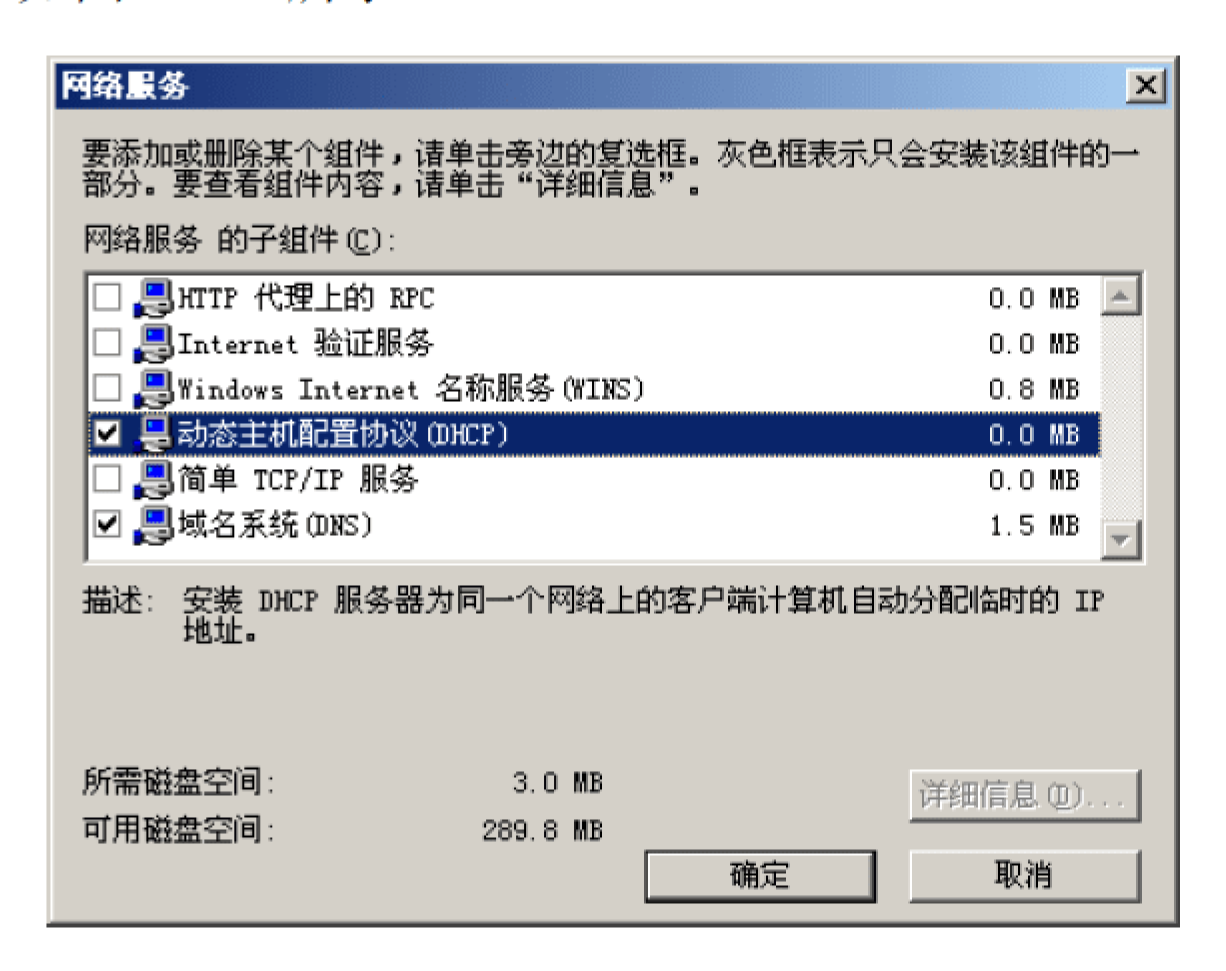


图 2-104 【网络服务】对话框

(3) 单击【下一步】按钮，将 Windows Server 2003 安装光盘放入光驱，即开始安装和配置 DHCP 组件。

(4) 安装完成后，单击【完成】按钮，返回到【添加/删除程序】对话框。单击【关闭】按钮即可完成 DHCP 服务的安装。

安装结束后，会在【开始】|【程序】|【管理工具】菜单中增加 DHCP 菜单项。

2. 添加 DHCP 服务器

在安装 DHCP 服务后，用户必须首先添加一个授权的 DHCP 服务器，并在服务器中添加作用域，设置相应的 IP 地址范围及选项类型，以便 DHCP 客户机在登录到网络时，能够获得 IP 地址租约和相关选项的设置参数。具体操作步骤如下。

(1) 选择【开始】|【程序】|【管理工具】| DHCP 命令，打开 DHCP 窗口，如图 2-105 所示。

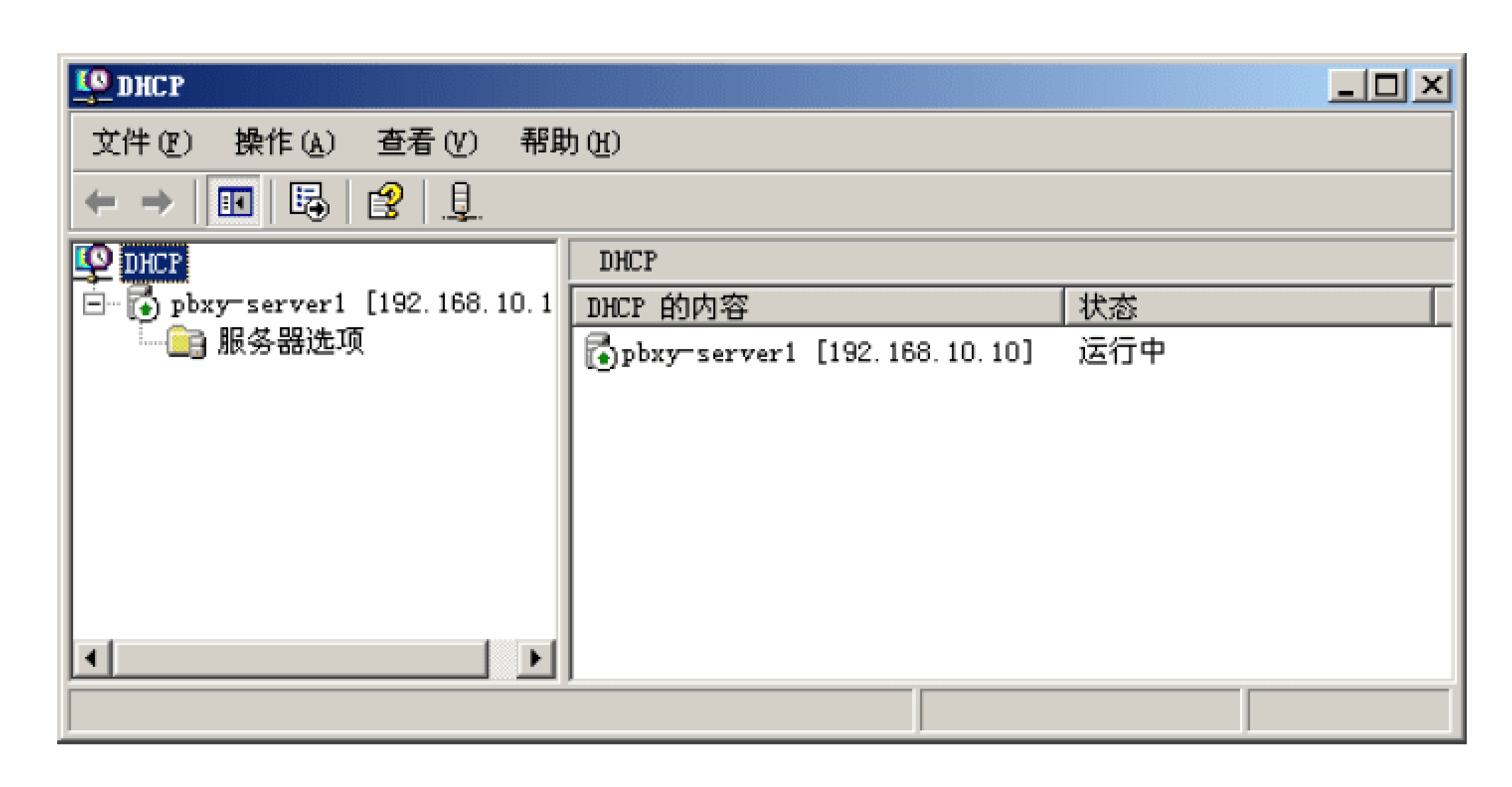


图 2-105　DHCP 控制台窗口

(2) 选择【操作】|【添加服务器】命令，打开【添加服务器】对话框，如图 2-106 所示。

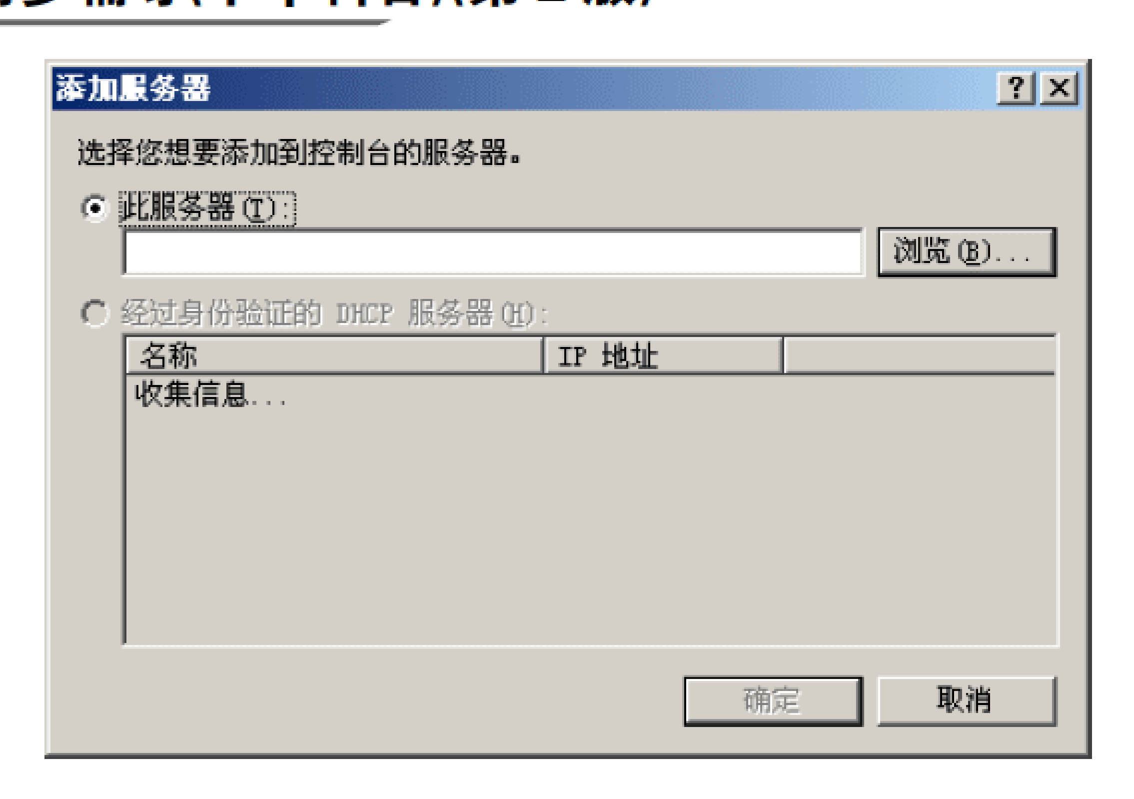


图 2-106 【添加服务器】对话框

(3) 在【此服务器】文本框中输入 DHCP 服务器名或 IP 地址，也可单击【浏览】按钮，在出现的对话框中选择要添加的 DHCP 服务器。

3. 授权 DHCP 服务器

用户只是简单地在 DHCP 控制台中添加一台 DHCP 服务器还不能使该服务器正常进行工作。在 DHCP 服务器为客户机动态地分配 IP 地址之前，用户还必须为新添加的服务器进行授权。这里的授权是指：为了保证网络的安全 Windows Server 2003 服务器系统只允许那些已经被授权的 DHCP 服务器在网络中发行 IP 地址；而没有被授权的 DHCP 服务器不能为客户机提供服务。如果用户是在 Active Directory 的主域控制器上安装 DHCP 服务，在用户第一次向 DHCP 控制台添加该服务时，服务器便会自动为新添加的 DHCP 服务器进行授权。不过，用户可以为该主域控制器同时授权多个 DHCP 服务器来为网络客户机提供服务。

1) 授权的概念

DHCP 服务器在网络上正确配置和授权使用时，将提供有用且已计划好的管理服务。但是，当错误配置或未授权的 DHCP 服务器被引入网络时，它可能会带来问题。例如，如果启动了未授权的 DHCP 服务器，它可能开始为客户机租用不正确的 IP 地址或者否认尝试更新当前地址租约的 DHCP 客户机。这些配置中的任何一个都可能导致启用 DHCP 的客户机产生更多的问题。例如，从未授权的服务器获取配置租约的客户机将找不到有效的域控制器，致使客户机难以成功登录到网络。

为避免在 Windows Server 2003 中出现这些问题，在它们为客户机提供服务之前需要管理员在网络中验证服务器是否合法。这样就可避免由于在错误网络上运行带有不正确或正确配置的 DHCP 服务器而导致的大多数意外破坏。

如果用户配置了 Active Directory，那么作为 DHCP 服务器运行的所有计算机在目录服务中获得授权及为客户机提供 DHCP 服务之前，必须是域控制器或者域成员服务器。

要将计算机授权为 DHCP 服务器，可使用下列处理步骤。

(1) 使用具有企业管理特权的帐户或者使用已获得委派可向企业的 DHCP 服务器授权的帐户登录到网络。在大多数情况下，最简单的方法是从用户要授权新 DHCP 服务器的计算机登录到网络。这可以确保已授权计算机的其他 TCP/IP 配置已在授权之前正确建立。通常，用户可以使用作为企业管理员组成员的帐户。当 NetServices 容器对象存储在 Active Directory 服务的企业根位置时，用户使用的帐户必须允许其有访问该对象的“完全控制”

权限。

(2) 启动 DHCP 控制台并选择作为 DHCP 服务器运行的计算机，该 DHCP 服务器是用户想在目录服务数据库中作为授权服务器添加的。如果本地计算机未获得授权，那么在启动 DHCP 控制台时，请选择【本地计算机】选项用于连接。如果网络上的另一台计算机获得授权，请选择【远程计算机】选项。

授权 DHCP 服务器时，服务器计算机被添加到在目录服务数据库中维护的授权 DHCP 服务器列表中。用户可通过使用 Active Directory 站点和服务控制台检查属性来验证服务器是否已被添加。这些属性位于【配置】项下，它是在企业根的下列文件夹位置中保存的全局容器。

2) 为创建的 DHCP 服务器授权

在理解了授权的作用之后，用户即可为添加的 DHCP 服务器进行授权的操作了，以便使该服务器具有分配动态 IP 地址的权限。

下面是对 DHCP 服务器授权的具体操作步骤。

(1) 打开 DHCP 控制台窗口，在控制台目录树中右击 DHCP 根节点，从弹出的快捷菜单中选择【管理授权的服务器】命令，打开【管理授权的服务器】对话框，如图 2-107 所示。

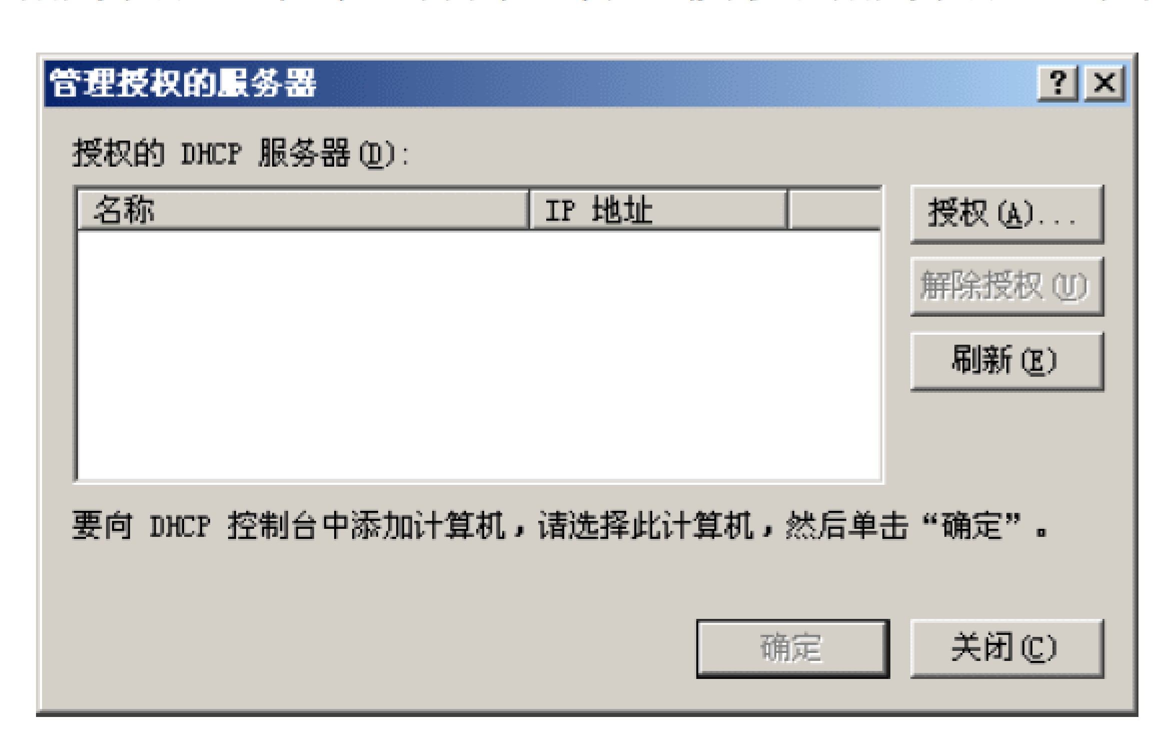


图 2-107 【管理授权的服务器】对话框

(2) 在【管理授权的服务器】对话框中，用户可以解除对已经被授权的 DHCP 服务器的授权，同时也可以为新的 DHCP 服务器进行授权。单击【授权】按钮后，系统将打开【授权 DHCP 服务器】对话框，如图 2-108 所示。

(3) 在【授权 DHCP 服务器】对话框中，用户需要在【名称或 IP 地址】文本框中输入刚添加的 DHCP 服务器的名称或 IP 地址，也可以输入本机的计算机名称。单击【确定】按钮后，系统将打开【确认授权】对话框，如图 2-109 所示。



图 2-108 【授权 DHCP 服务器】对话框



图 2-109 【确认授权】对话框

(4) 在该对话框中，系统将显示出用户指定的主机的名称及该主机的 IP 地址信息，以

使用户确认将要授权的 DHCP 服务器的正确性。单击【确定】按钮，系统将返回到【管理授权的服务器】对话框。授权的 DHCP 服务器已经被加入到了【授权的 DHCP 服务器】列表框中，单击【关闭】按钮即可。

4. 创建作用域

在创建了 DHCP 服务器并为其授权后，用户还需要进行另一项重要的工作，即创建作用域。作用域是指指派给请求动态 IP 地址的计算机的 IP 地址的范围。用户只有在创建了一个新的作用域后，DHCP 服务器才能拥有可被分配的 IP 地址，而这些地址都储存在地址池中。当客户机发出地址请求后，DHCP 服务器将与客户机签订一个地址租约，这样客户机将会以租借的形式来使用临时的 IP 地址。

1) 作用域概述

作用域是对使用 DHCP 服务的子网进行的计算机管理性分组。管理员首先为每个物理子网创建作用域，然后使用该作用域定义由客户机使用的参数。作用域具有下列属性。

- IP 地址的范围：可在其中加入或排除用于 DHCP 服务租约的地址。
- 惟一的子网掩码：用于确定给定 IP 地址的子网。
- 租约期限：指派给动态接收分配的 IP 地址的 DHCP 客户机。

2) 创建作用域的过程

DHCP 作用域由给定子网上 DHCP 服务器可以租用给客户机的 IP 地址池组成。例如，213.248.173.113～213.248.173.129。每个子网只能有一个具有连续 IP 地址范围的单个 DHCP 作用域。要在单个作用域或子网内使用多个地址范围以提供 DHCP 服务，必须首先定义作用域，然后设置所需的任何排除范围。

管理员应该在不希望 DHCP 服务器提供或用于 DHCP 指派的作用域中设置任何 IP 地址排除范围。例如，可通过创建 168.168.168.1～168.168.168.22 的排除范围，将其中的 10 个地址排除在外。通过为这些地址设置排除范围，可以指定在从服务器上请求租用配置时永远不为 DHCP 客户机提供这些地址。排除的 IP 地址可能是网络上的有效地址，但这些地址只能是通过在不使用 DHCP 获取地址的主机上手动配置的。

定义作用域以后，用户可通过另外配置作用域，以排除不必租给 DHCP 客户机的任何其他 IP 地址。应该为所有必须静态配置的设备使用排除范围。排除范围应包含管理员手动指派给其他 DHCP 服务器、非 DHCP 客户机、无盘工作站或者路由和远程访问及 PPP 客户机的所有 IP 地址。也可以选择为网络上的指定计算机或设备的永久租约指派保留某些 IP 地址。

创建作用域的主要作用是为服务器指定和配置好可分配的 IP 地址。因此，在创建新的 DHCP 服务器的操作中创建作用域的工作至关重要，它关系到 DHCP 是否拥有可分配的 IP 地址。

下面介绍创建 DHCP 作用域的操作步骤。

(1) 打开 DHCP 窗口，在控制台树中右击要创建作用域的 DHCP 服务器，从弹出的快捷菜单中选择【新建作用域】命令，打开【新建作用域向导】对话框，如图 2-110 所示。

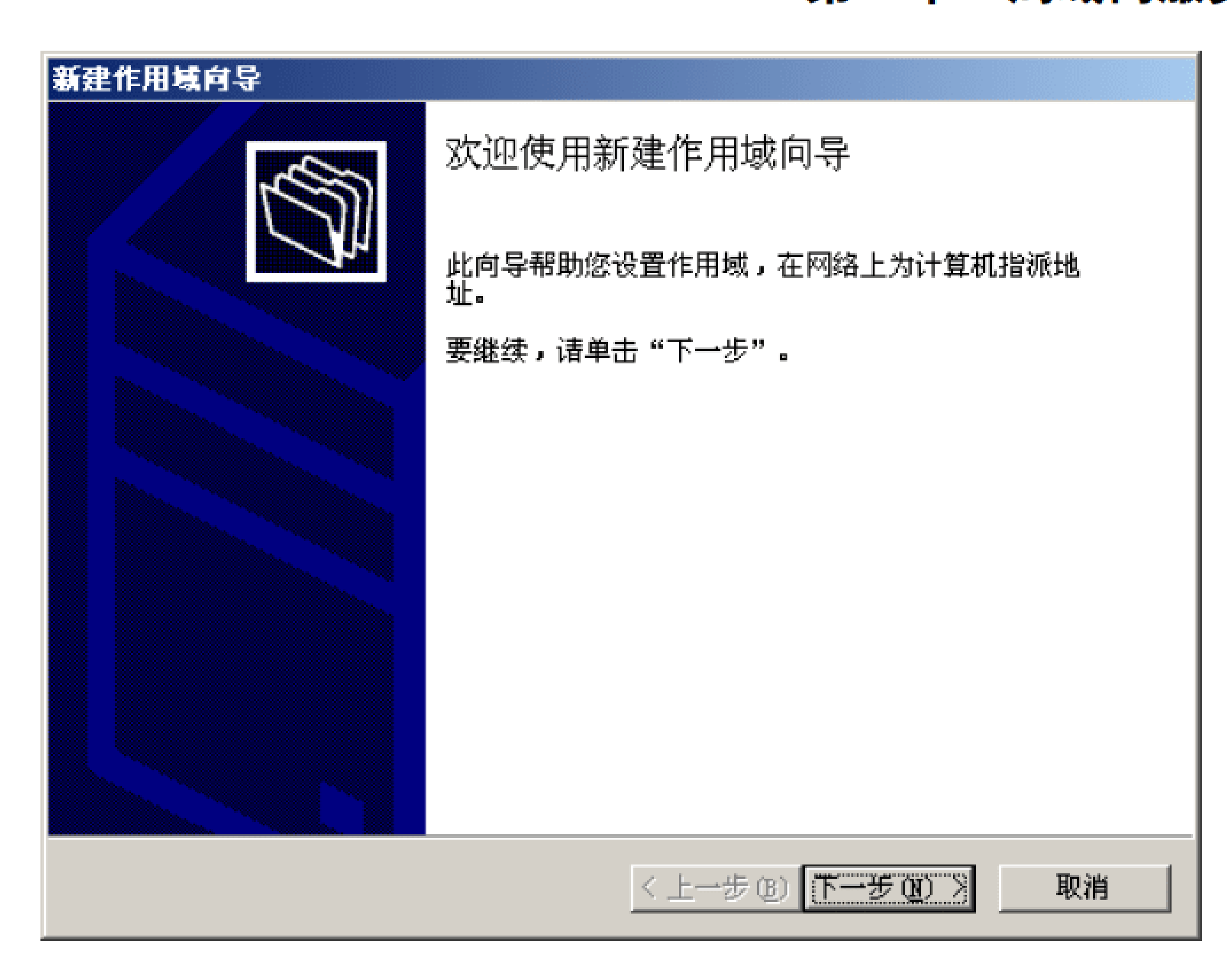


图 2-110 【新建作用域向导】对话框

(2) 单击【下一步】按钮，系统将打开【作用域名】界面。在该对话框中，用户需要在【名称】文本框中输入作用域的名称，并在【描述】文本框中输入一些说明性文字，如图 2-111 所示。

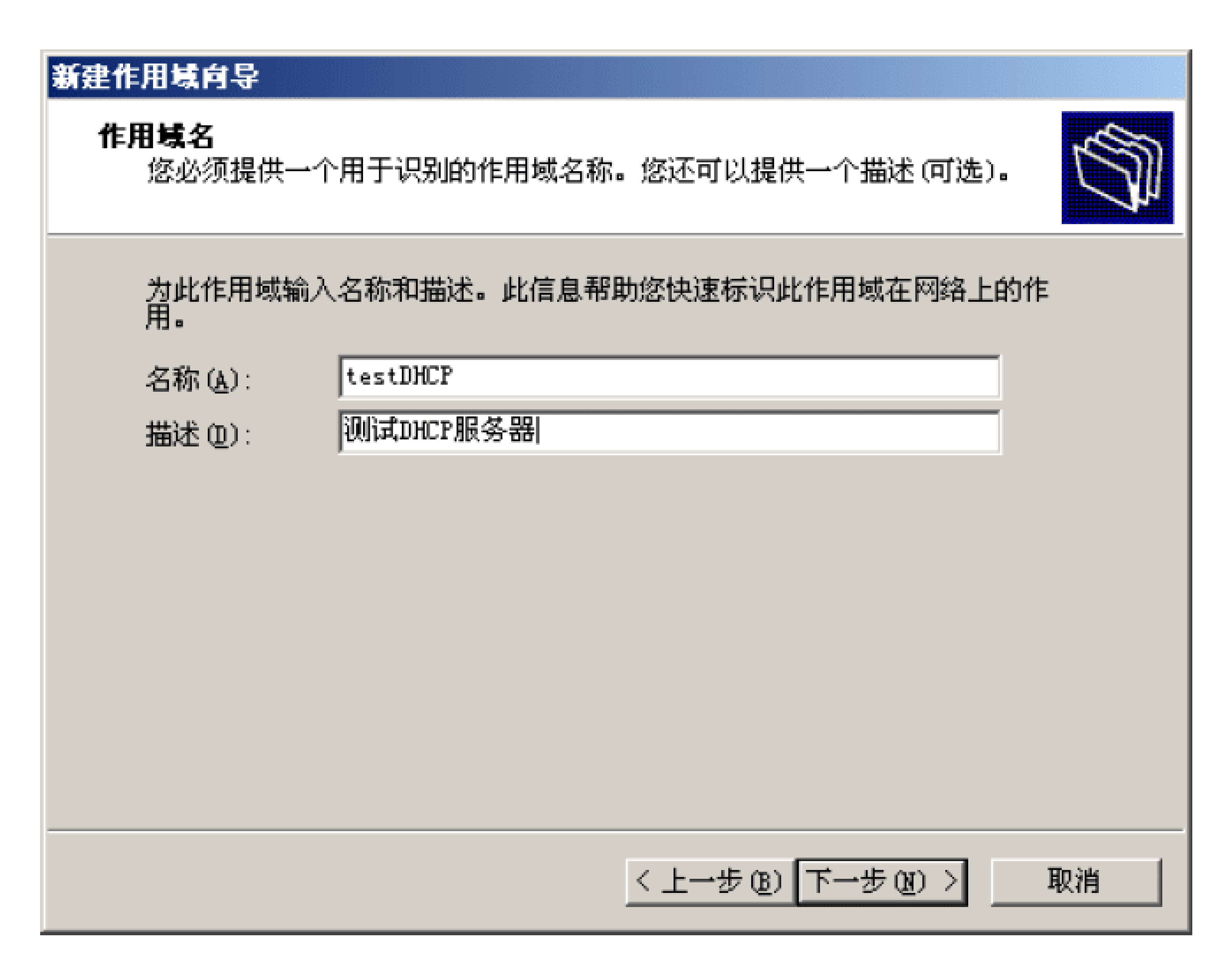


图 2-111 【作用域名】界面

(3) 单击【下一步】按钮后，系统将打开【IP 地址范围】界面。在该界面中，用户可以指定作用域的地址范围。在【输入此作用域分配的地址范围】选项区域的【起始 IP 地址】和【结束 IP 地址】文本框中分别输入作用域的起始地址和结束地址。通过输入合适的子网掩码，用户可以调整已定义的 IP 地址中有多少位用作网络的 ID 及多少位用作主机的 ID。不同的子网掩码决定了网络客户机属于不同的网络。同时用户还可以通过调整【长度】文本框的数值来完成子网掩码的设置，如图 2-112 所示。

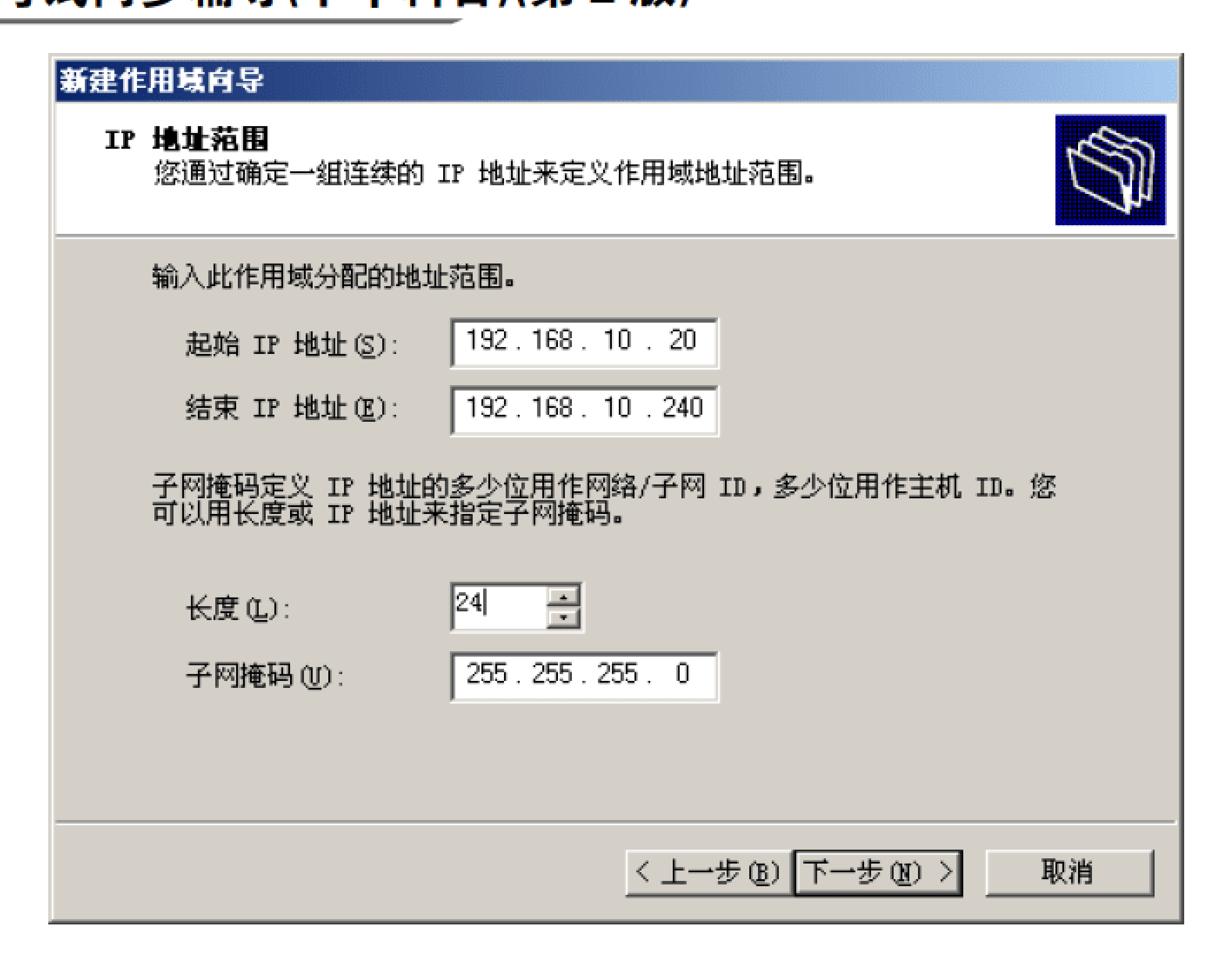


图 2-112 【IP 地址范围】界面

(4) 单击【下一步】按钮进入【添加排除】对话框，如图 2-113 所示。在该界面中，用户可以定义服务器不分配的 IP 地址。排除范围应当包括所有手工分配给其他 DHCP 服务器、非 DHCP 客户机、无盘工作站或 RAS 和 PPP 客户机的 IP 地址。如果有要排除的 IP 地址，按下述方法定义。

新建作用域向导
添加排除
排除是指服务器不分配的地址或地址范围。
键入您想要排除的 IP 地址范围。如果您想排除一个单独的地址，则只在“起始 IP 地址”键入地址。
起始 IP 地址(S): 192 . 168 . 10 . 200
结束 IP 地址(E):
添加(D)
排除的地址范围(C):
192.168.10.100 到 192.168.10.120
删除(V)
< 上一步(B)
下一步(N) >
取消

图 2-113 【添加排除】界面

在【起始 IP 地址】文本框中输入排除范围的 IP 起始地址，在【结束 IP 地址】文本框中输入排除范围的 IP 结束地址，然后单击【添加】按钮。如果有多个排除范围，使用同样的方法定义它们。

要排除单个 IP 地址，只需在【起始地址】文本框中输入该 IP 地址，而【结束地址】文本框保持为空，然后单击【添加】按钮即可。

要从排除范围中删除 IP 地址或 IP 地址范围，在【排除的地址范围】列表框中单击该地址，然后单击【删除】按钮即可。

(5)　单击【下一步】按钮，进入【租约期限】界面。租约期限指定了客户机使用 DHCP 服务器所分配的 IP 地址的时间。要指定作用域中 IP 地址的租用时间，可通过微调框定义 IP 地址租用时间的“天”、“小时”和“分钟”数值，如图 2-114 所示。

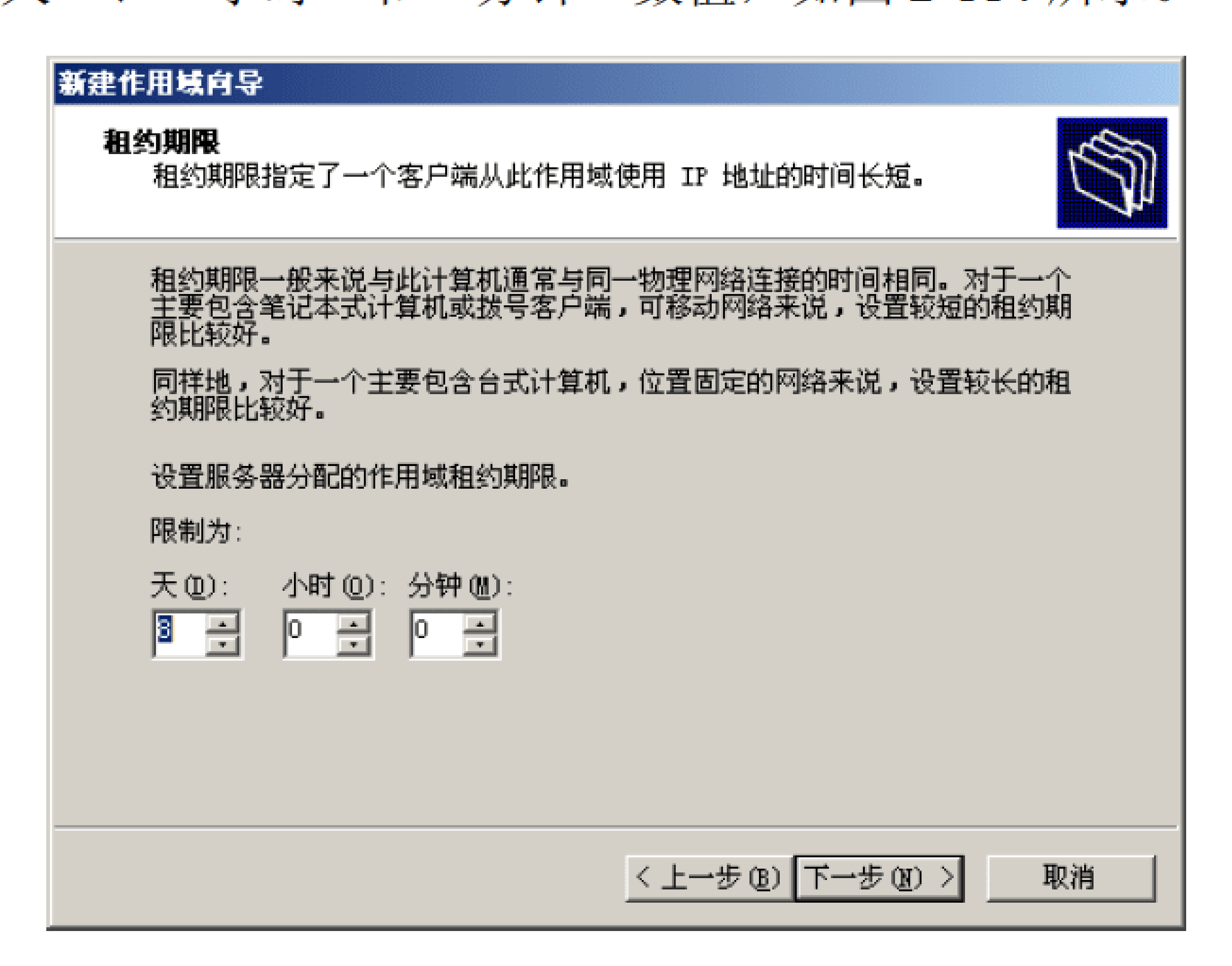


图 2-114　【租约期限】界面

(6)　单击【下一步】按钮，将打开【配置 DHCP 选项】界面。要想让网络客户使用作用域，必需配置最常用的 DHCP 选项，这些选项包括网关、DNS 服务器和 WINS 设置等。要想立即配置这些 DHCP 选项，可选中【是，我想现在配置这些选项】单选按钮，如图 2-115 所示。

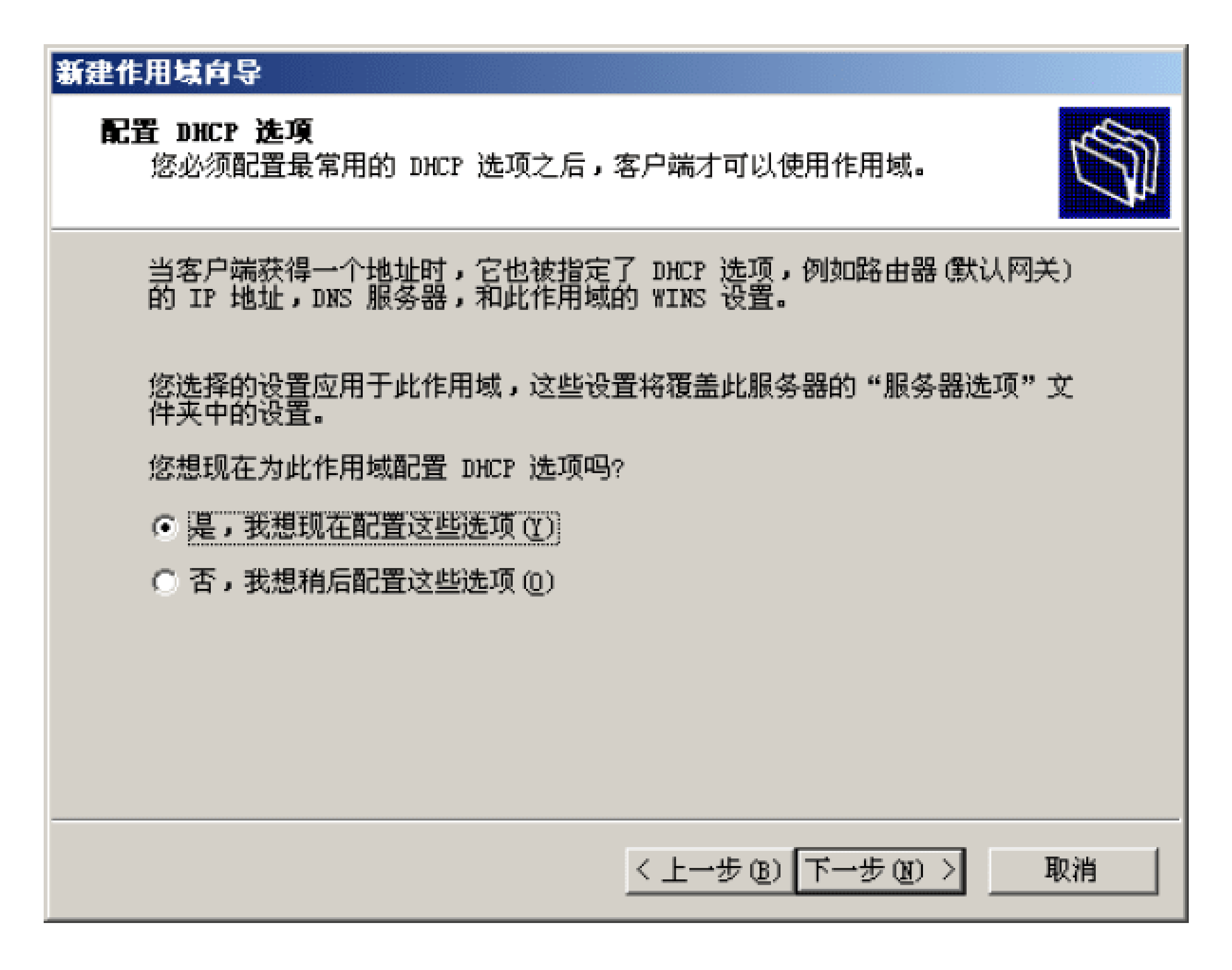


图 2-115　【配置 DHCP 选项】界面

(7)　单击【下一步】按钮，在打开的【路由器(默认网关)】界面中可配置作用域的网关(或路由器)。在【IP 地址】文本框中输入网关地址，然后单击【添加】按钮添加网关。要删除已有的网关，可在网关列表框中单击该网关地址，然后单击【删除】按钮即可。如果管理员所在的网络不需要路由器，可以直接单击【下一步】跳过该步操作，如图 2-116 所示。

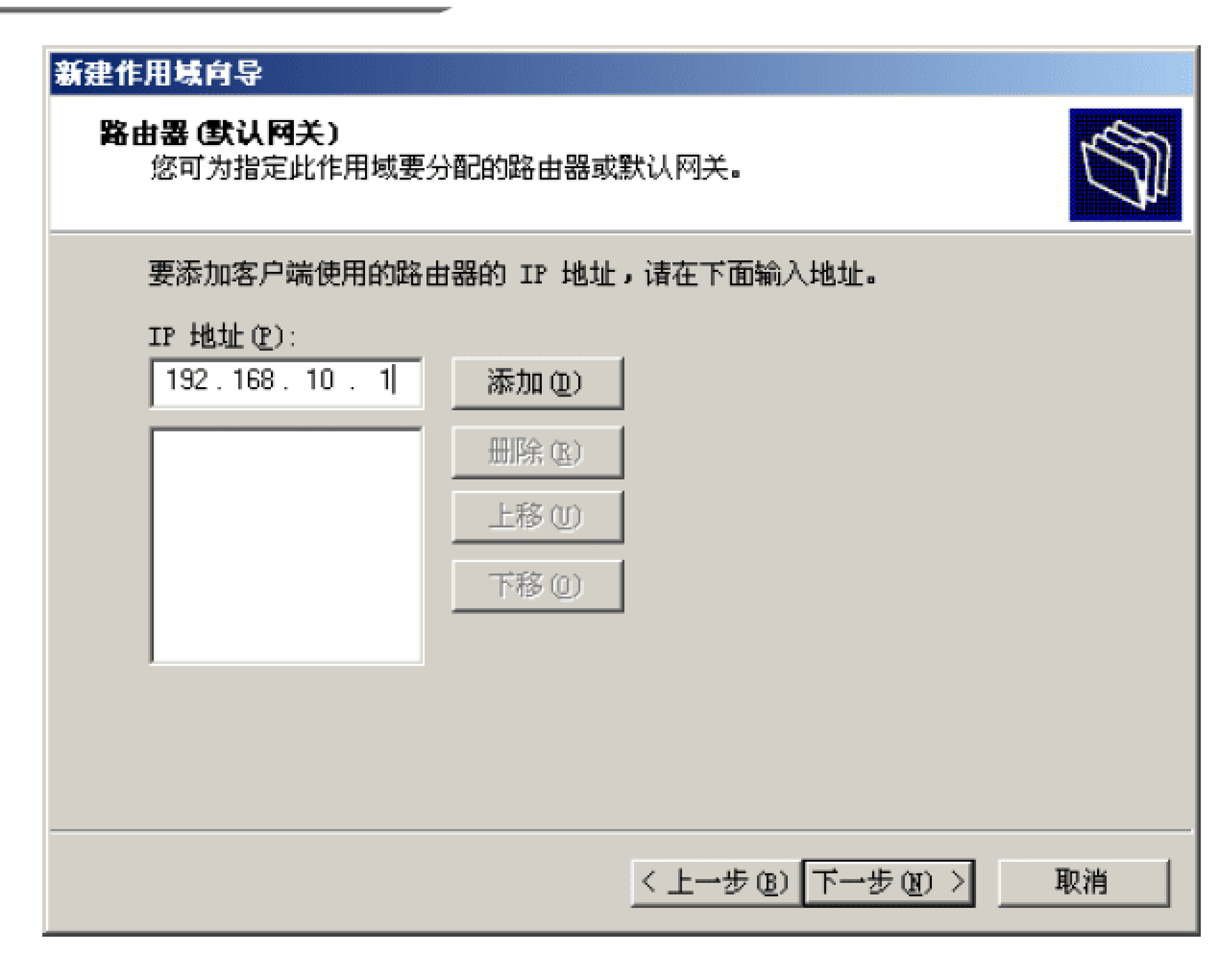


图 2-116 【路由器(默认网关)】界面

(8) 单击【下一步】按钮，将打开【域名称和 DNS 服务器】界面。在【父域】文本框中，需要输入父域的名称。如果本机为根域的控制器而没有父域存在，可以直接输入本地域名。

在【服务器名】文本框中输入本地 DNS 服务器的名称后单击【解析】按钮，系统会将已经配置的 DNS 服务器的 IP 地址显示在【IP 地址】文本框中。用户只需单击【添加】按钮即可将该地址加入到 DNS 服务器列表中，如图 2-117 所示。

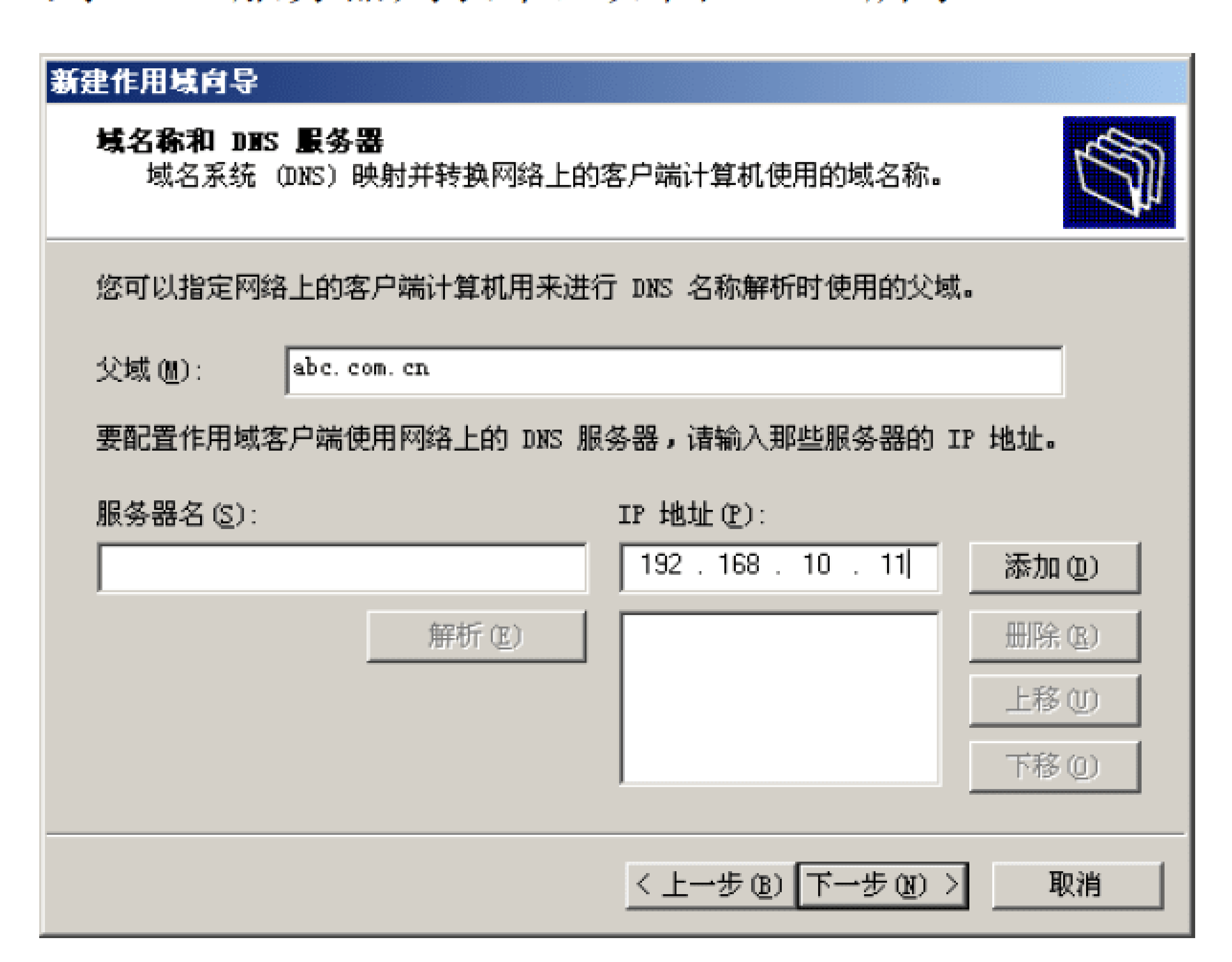


图 2-117 【域名称和 DNS 服务器】界面

(9) 单击【下一步】按钮，系统将打开【WINS 服务器】界面。在该界面中，用户可以输入 WINS 服务器地址。WINS 服务器可以将 Windows 客户的计算机名称转换成相应的 IP 地址。单击【解析】按钮后，系统将该 WINS 服务器对应的 IP 地址显示在【IP 地址】文本框中，最后单击【添加】按钮将该地址加入到地址列表中，如图 2-118 所示。

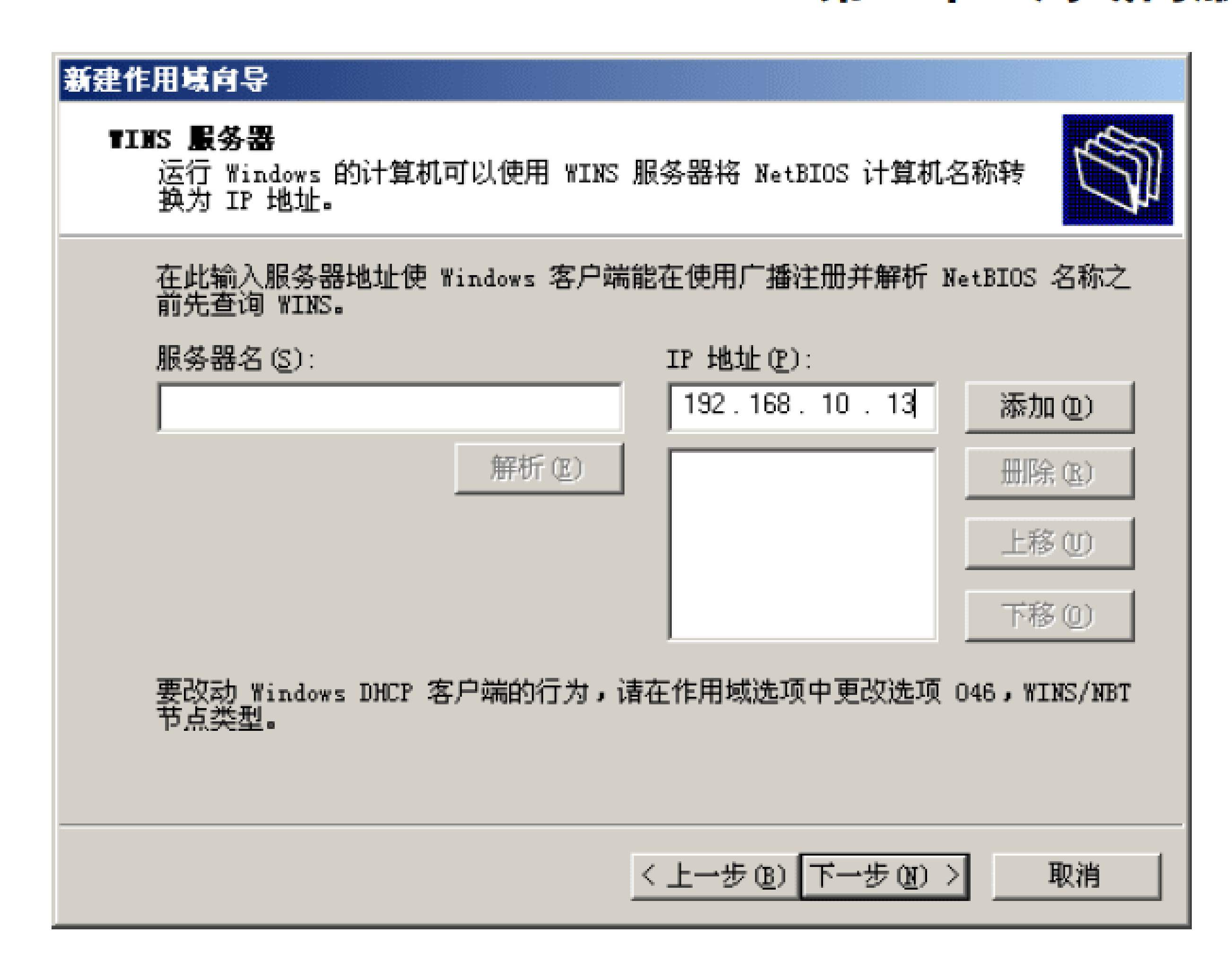


图 2-118　【WINS 服务器】界面

(10) 完成 WINS 服务器设置后，单击【下一步】按钮，打开【激活作用域】界面，从中选中【是，我想现在激活此作用域】单选按钮，如图 2-119 所示。单击【下一步】按钮，可立即激活此作用域。这样创建作用域向导就完成了创建过程。最后系统将打开【正在完成新建作用域向导】界面，单击【完成】按钮即可。



图 2-119　【激活作用域】界面

注意：如果用户在创建作用域时没有很好地设置其内容，可在作用域创建之后，通过其属性对话框来修改设置。但是，在修改地址范围时一般不应缩小其地址范围，因为缩小地址范围可能导致 DHCP 客户租约地址的失败。

5. 配置作用域

用户在创建了新的作用域后，还需要对作用域选项进行一些相关的配置才能正常启动作用域中众多的选项功能。

1)　设置作用域选项

要配置作用域选项，可参照下面的操作步骤。

(1) 选择【开始】|【程序】|【管理工具| DHCP 命令，打开 DHCP 控制台。在目录树中单击服务器节点并展开【作用域】节点及其子节点。右击选定的【作用域选项】节点，从弹出的快捷菜单中选择【配置选项】命令，打开【作用域选项】对话框并切换到【常规】选项卡，如图 2-120 所示。

(2) 在【可用选项】列表框中，当用户选中了某选项时，系统将自动在【数据输入】选项区域中打开该选项对应的设置。例如，选中【006 DNS 服务器】复选框后，在【数据输入】选项区域中系统会让用户输入名称服务器的新 IP 地址及服务器名称。用户在【IP 地址】文本框中输入新的 IP 地址，然后单击【添加】按钮将该地址添加到名称服务器列表中。用户也可以在【服务器名】文本框中输入某台服务器的名称，然后单击【解析】按钮，系统会自动将该服务器对应的 IP 地址解析到【IP 地址】文本框中。

(3) 用户对所选定的作用域选项进行正确设置后，单击【确定】按钮以使设置生效。

(4) 对常规选项设置完毕后，单击【高级】标签，切换到【高级】选项卡，如图 2-121 所示。

(5) 在【高级】选项卡中，可以对作用域的高级选项进行配置。其中在【供应商类别】下拉列表框中，用户可以在【DHCP 标准选项】、【Microsoft 98 选项】、【Microsoft 2000 选项】和【Microsoft 选项】4 种选项中选择其中一种。当选择了一种供应商类别后，其对应的可选项将显示在【可用选项】列表框中。如果用户已创建了 DHCP 服务器以及作用域的话，在【用户类别】下拉列表框中，系统会默认设置该选项为【默认用户类别】。

(6) 如同在【常规】选项卡中的设置操作一样，在【可用选项】列表框中选定某选项后，可在【数据输入】选项区域中对该选项进行相应的设置。

(7) 完成所有设置后，单击【确定】按钮以使设置生效。

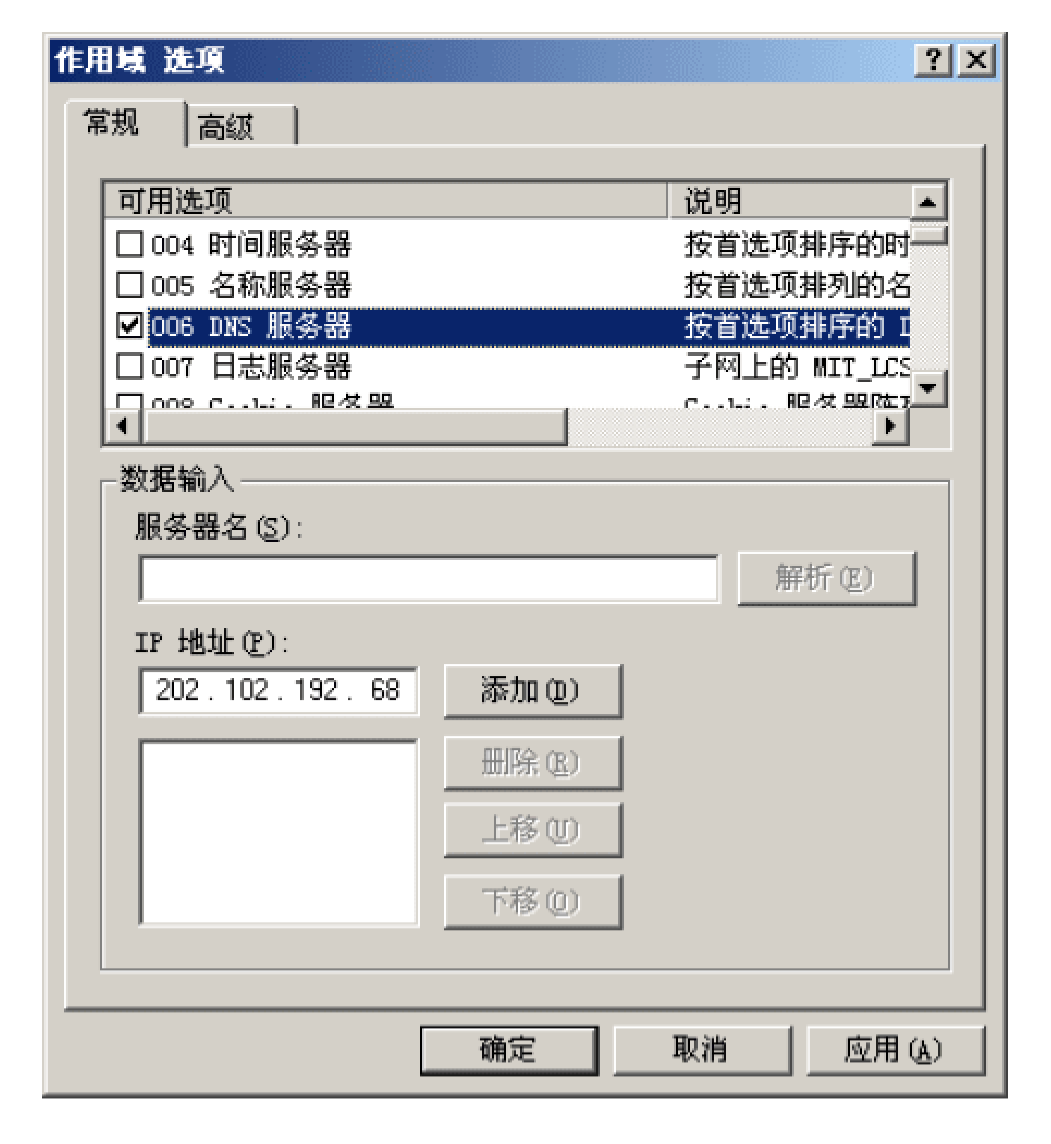


图 2-120 【常规】选项卡

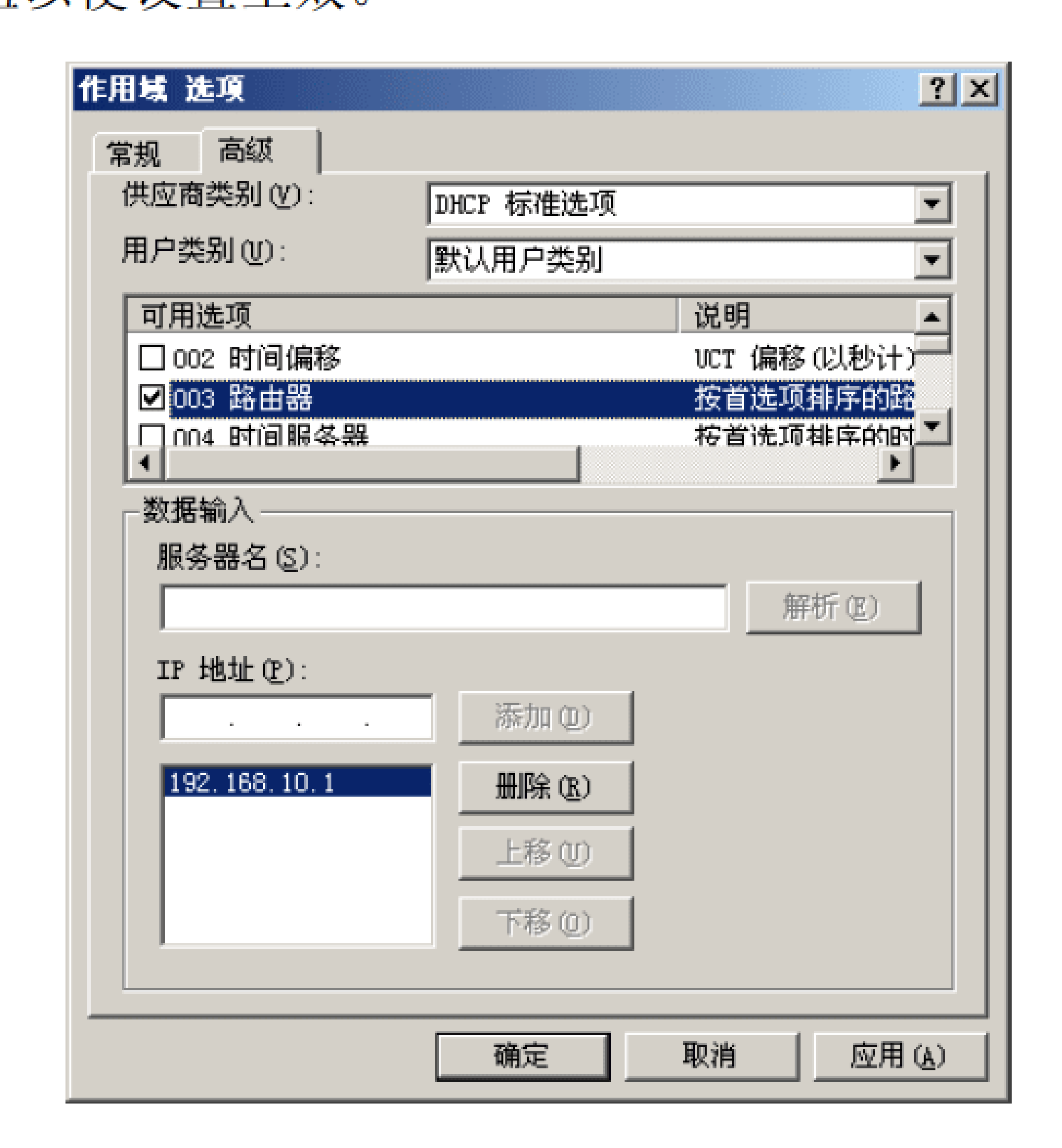


图 2-121 【高级】选项卡

2) 保留特定 IP 地址

有些时候，在 DHCP 网络中需要给某一台或几台 DHCP 客户端固定专用的 IP 地址，这就需要通过 DHCP 服务器提供的“保留”功能来实现。当这个 DHCP 客户端每次向 DHCP

服务器请求获得 IP 地址或更新 IP 地址租期时，DHCP 服务器都会给该 DHCP 客户端分配同一个 IP 地址。保留特定 IP 地址的操作步骤如下。

(1) 选择【开始】|【程序】|【管理工具】| DHCP 命令，打开 DHCP 控制台。在目录树中单击服务器节点并展开【作用域】节点及其子节点。右击【保留】节点，从弹出的快捷菜单中选择【新建保留】命令，打开【新建保留】对话框，如图 2-122 所示。

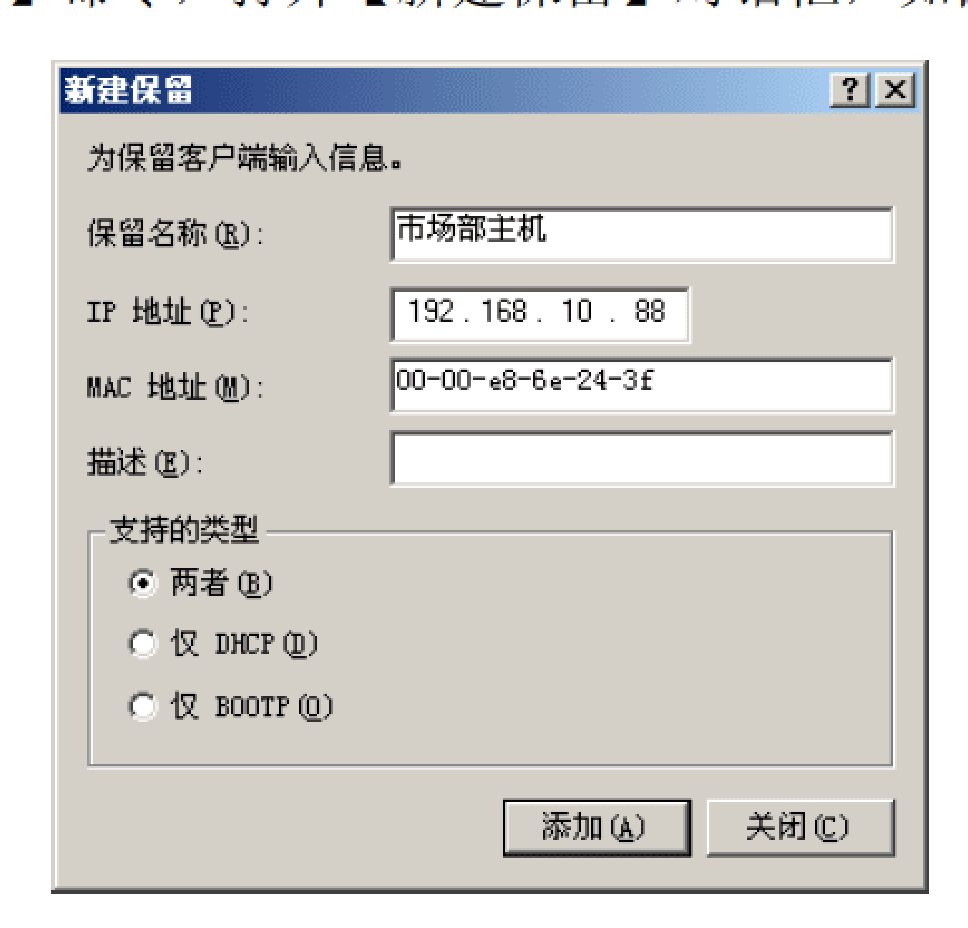


图 2-122 【新建保留】对话框

(2) 在【新建保留】对话框中输入保留名称、IP 地址、MAC 地址、说明并选择支持的类型。

在【保留名称】文本框中输入用于标识 DHCP 客户端的名称，该项既可以是 DHCP 客户端的真实名称，也可以是自定义的名称；在【IP 地址】文本框中输入要保留给该 DHCP 客户端的 IP 地址；在【MAC 地址】文本框中输入该 DHCP 客户端网卡的 MAC 地址。网卡的 MAC 地址是一个 12 位十六进制数，每块网卡地址是惟一的，它一般在出厂时标注在网卡上。在 Windows 95/98/Me 计算机上，可以利用 Winipcfg 测试工具测得；在 Windows NT/2000/XP/2003 系统的客户端，需要进入 DOS 提示符下，输入 ipconfig/all 命令来获得。【描述】文本框用于在必要时输入一些辅助说明性文字；【支持的类型】用于设置该客户端是否必须支持 DHCP 服务。其中 BOOTP 主要用于无盘工作站，因此如果该客户端是以无盘方式工作，则选中【仅 BOOTP】单选按钮；否则选中【仅 DHCP】单选按钮。当无法确定时可以选中【两者】单选按钮。

(3) 输入完毕后，单击【添加】按钮可以保留一个 IP 地址给特定 DHCP 客户端来使用。

3) 协调作用域

协调作用域信息就是要协调 DHCP 数据库中的作用域信息与注册表中的相关信息，使其保持一致。如果不一致，系统将提示管理员修复错误将其协调一致，以免出现地址分配错误。

下面是协调作用域的操作步骤。

(1) 打开 DHCP 控制台窗口，在控制台树中展开要协调作用域的服务器。右击要协调的作用域，从弹出的快捷菜单中选择【协调】命令，打开【协调】对话框，如图 2-123 所示。

(2) 在【协调】对话框中，单击【验证】按钮即可将数据库中的作用域信息与注册表中的信息比较，如果一致，则会出现一个 DHCP 对话框，单击【确定】按钮即可，如图 2-124



所示。

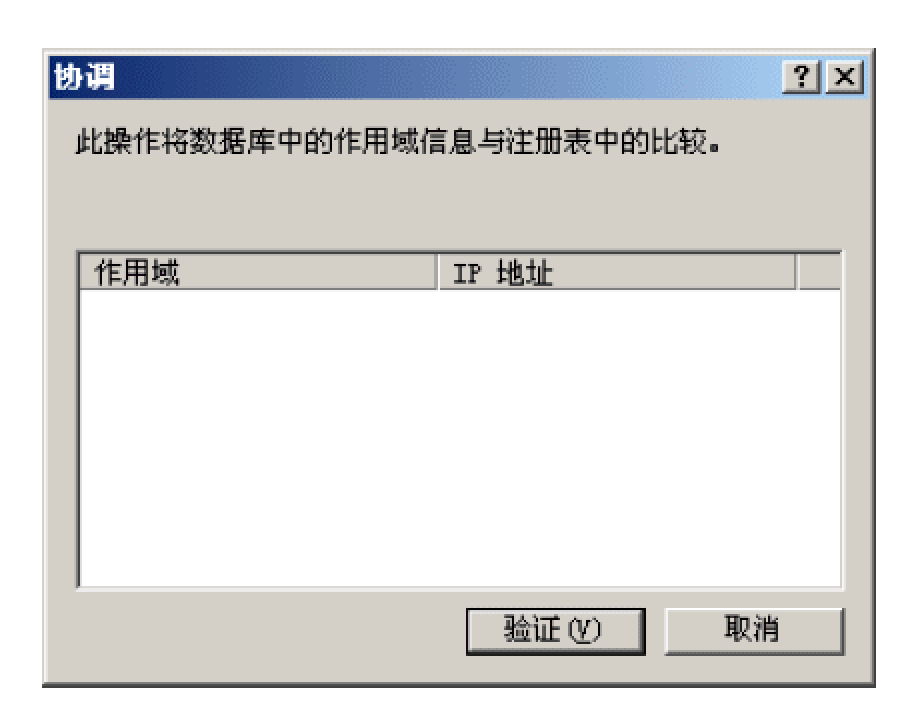



图 2-123　协调作用域



图 2-124　协调作用域结果

(3) 如果作用域不一致，在列表框中就会列出所有不一致的 IP 地址，且【验证】按钮变为【协调】按钮。要修复不一致性，可先选择需要协调的 IP 地址，然后单击【协调】按钮即可。

(4) 单击【确定】按钮关闭对话框。

注意： 上面所讲是对单个作用域进行协调，如果某个服务器有多个作用域，管理员也可以同时对它们进行协调。方法是：右击要协调的服务器，从弹出的快捷菜单中选择【协调所有的作用域】命令，打开【协调所有的作用域】对话框，然后按照上面的方法进行验证和协调即可。

4) 删除作用域

删除作用域就是从 DHCP 服务器中彻底地清除作用域中的 IP 地址对 DHCP 客户的分配。但是，删除作用域之前请务必停用作用域足够长的时间，以便能将客户机转移到不同的作用域。一旦所有客户机均已移动或强制在另一个作用域中搜索，管理员就可以安全地删除非活动的作用域。

要删除作用域，用户可以打开 DHCP 控制台窗口，在控制台目录树中展开所需服务器，右击要删除的作用域，从弹出的快捷菜单中选择【删除】命令即可。

6. 创建超级作用域

在 Windows Server 2003 中，用户除了可以使用 DHCP 服务器中标准的作用域来进行地址分配和地址管理外，还可以使用超级作用域来更好地分配和管理网络地址。因为，超级作用域允许用户将几个不同的作用域在逻辑上组合在一起并使用单一的作用域名称，这样用户就可以通过超级作用域对多个逻辑网进行管理。

1) 超级作用域的概念

超级作用域是 Windows Server 2003 中 DHCP 服务器的管理功能，它可以通过 DHCP 控制台创建和管理。使用超级作用域，可以将多个作用域组合为单个管理实体。使用此功能，DHCP 服务器可以在使用多个逻辑 IP 网络的单个物理网段(如单个以太网的局域网段)支持 DHCP 客户机。在每个物理域网或网络上使用多个逻辑 IP 网络时，这种配置通常被称为多网。它还能支持位于 DHCP 和 BOOTP 中继代理远端的远程 DHCP 客户机，并在中继代理

远端的网络上使用多网配置。

在全网配置中，可以使用 DHCP 超级作用域来组合并激活网络上使用的单独作用域范围内的 IP 地址。这种情况下，DHCP 服务器计算机可以为单个物理网络上的客户机激活并提供来自多个作用域的租约。

超级作用域可以解决多网结构中的某种 DHCP 配置问题。例如，当前活动作用域的可用地址池几乎已耗尽，需要向网络中添加更多的计算机。最初的作用域包括指定地址类别的单个 IP 网络的一段完全可寻址范围，需要使用另一个网络地址范围以扩展同一物理网段的地址空间。

2)　创建超级作用域

由于超级作用域可以包含其他分离的作用域的 IP 地址，所以当管理员需要使用另外一个 IP 网络地址范围以扩展同一个物理网段的地址空间时，就可以通过创建超级作用域来解决问题。

注意：　服务器要至少包含一个已创建的作用域，新建超级作用域的命令才能使用。

要创建超级作用域，可以参考以下步骤。

(1)　打开 DHCP 控制台窗口，在控制台目录树中单击想要创建超级作用域的 DHCP 服务器。选择【操作】菜单中的【新建超级作用域】命令，打开【新建超级作用域向导】对话框，如图 2-125 所示。

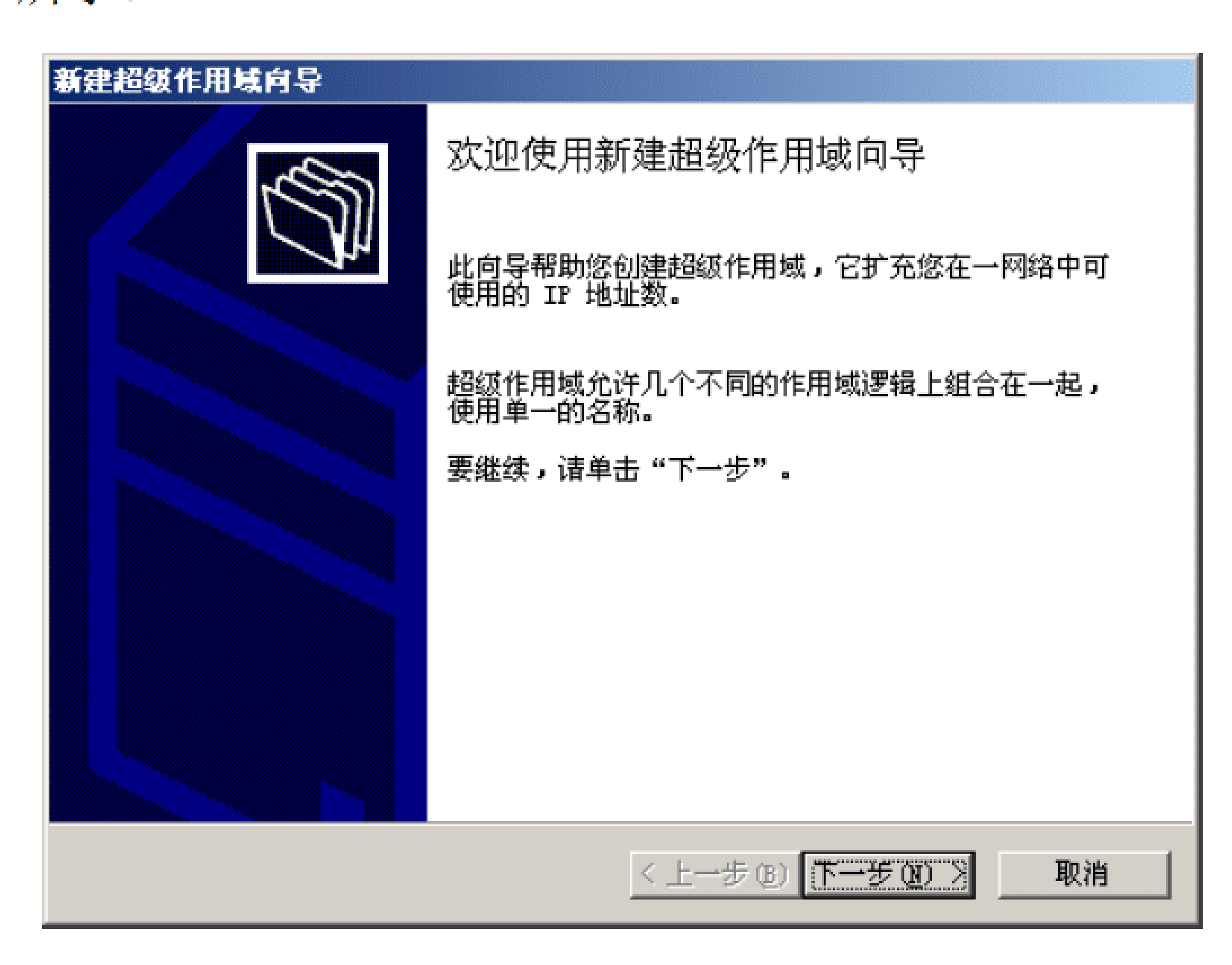


图 2-125　【新建超级作用域向导】对话框

(2)　在打开的【超级作用域名】界面中输入超级作用域的名称，如图 2-126 所示。

(3)　单击【下一步】按钮，打开【选择作用域】界面，如图 2-127 所示，在该界面中可选择该超级作用域所要包含的成员作用域(或称子作用域)。在【可用作用域】列表中选择作用域时，如果需要选择多个作用域，可在按下 Shift 键的同时单击作用域来选择多个连续作用域，或在按下 Ctrl 键的同时单击作用域来选择多个不连续作用域。

(4)　单击【下一步】按钮，系统将打开【创建完成】界面，显示出所设置的作用域选项，单击【完成】按钮即可完成创建过程。



图 2-126 【超级作用域名】界面



图 2-127 【选择作用域】界面

7. 设置 DHCP 服务器的属性

配置一台 DHCP 服务器的属性在创建该服务器的整个过程中是最关键的一步工作。合适的属性配置能够保证该服务器正常、顺利地运行，也只有这样，DHCP 服务器才能对客户机的地址请求做出应答——为客户机分配一个可用的动态 IP 地址。对 DHCP 服务器的属性中一些关键的项目进行合理设置是用户最后完成创建一台 DHCP 服务器的必要工作。

下面将介绍如何对 DHCP 服务器的属性进行设置。

1) 设置【常规】选项卡

(1) 打开【开始】菜单，选择【管理工具】| DHCP 命令，打开 DHCP 控制台窗口。右击选定的服务器，从弹出的快捷菜单中选择【属性】命令，打开该服务器的属性对话框，如图 2-128 所示。

(2) 在【常规】选项卡中，可以选中【自动更新统计信息间隔】复选框，然后通过【小时】和【分钟】微调按钮任意调整统计信息的刷新时间间隔的数值。这样 DHCP 服务器将

按用户设定的时间间隔数值自动统计信息。

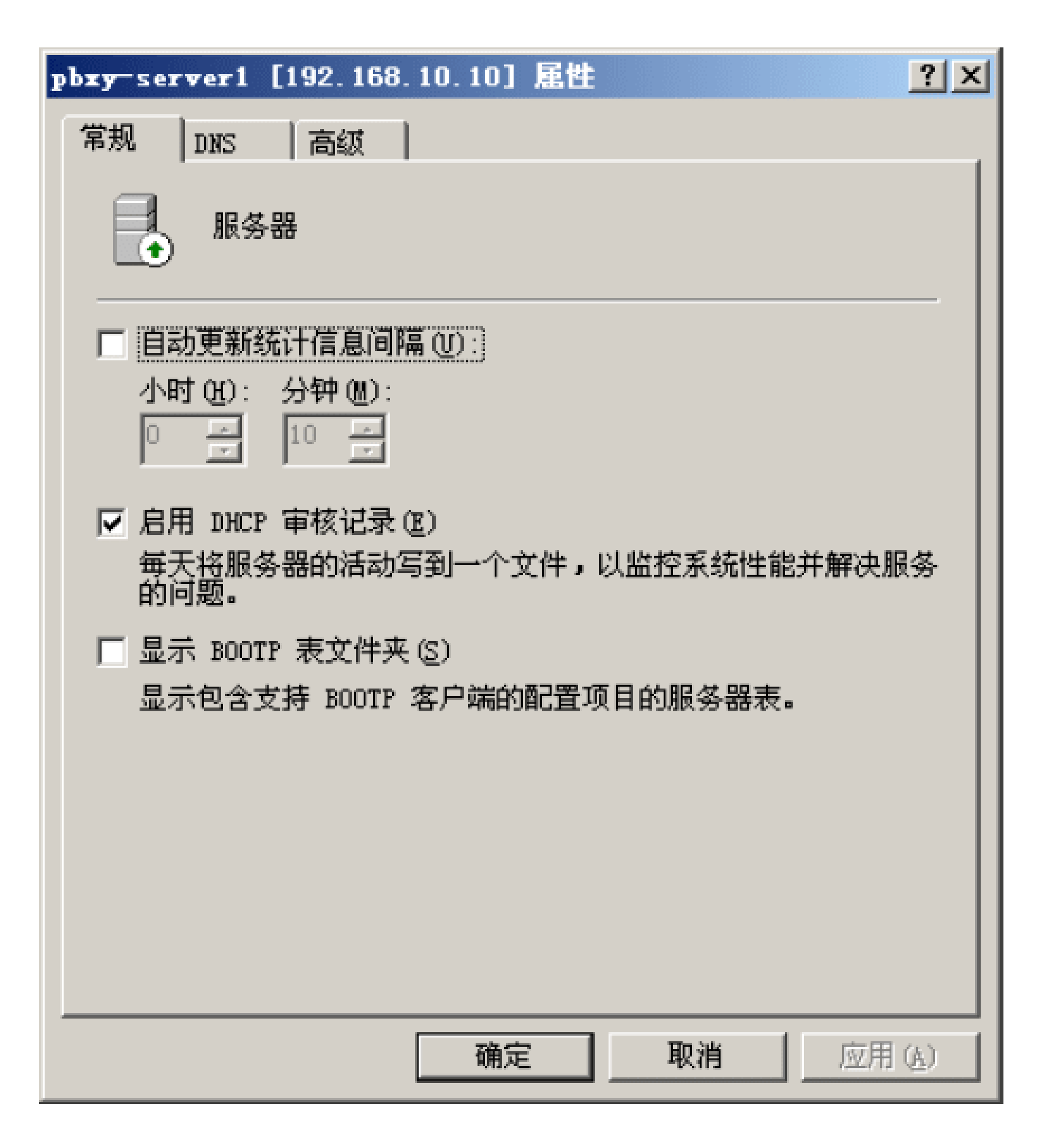


图 2-128　DHCP 服务器的属性对话框

(3)　如果用户希望启用 DHCP 日志记录，使该日志记录每天都将服务器的活动记录到一个文件中以供解答用户有关服务的疑难问题，可以选中【启用 DHCP 审核记录】复选框。另外，如果选中【显示 BOOTP 表文件夹】复选框，可以使用户在 DHCP 控制台窗口中查看到 BOOTP 文件夹消息。

2)　设置 DNS 选项卡

(1)　在选定的 DHCP 服务器的【属性】对话框中打开 DNS 选项卡，如图 2-129 所示。

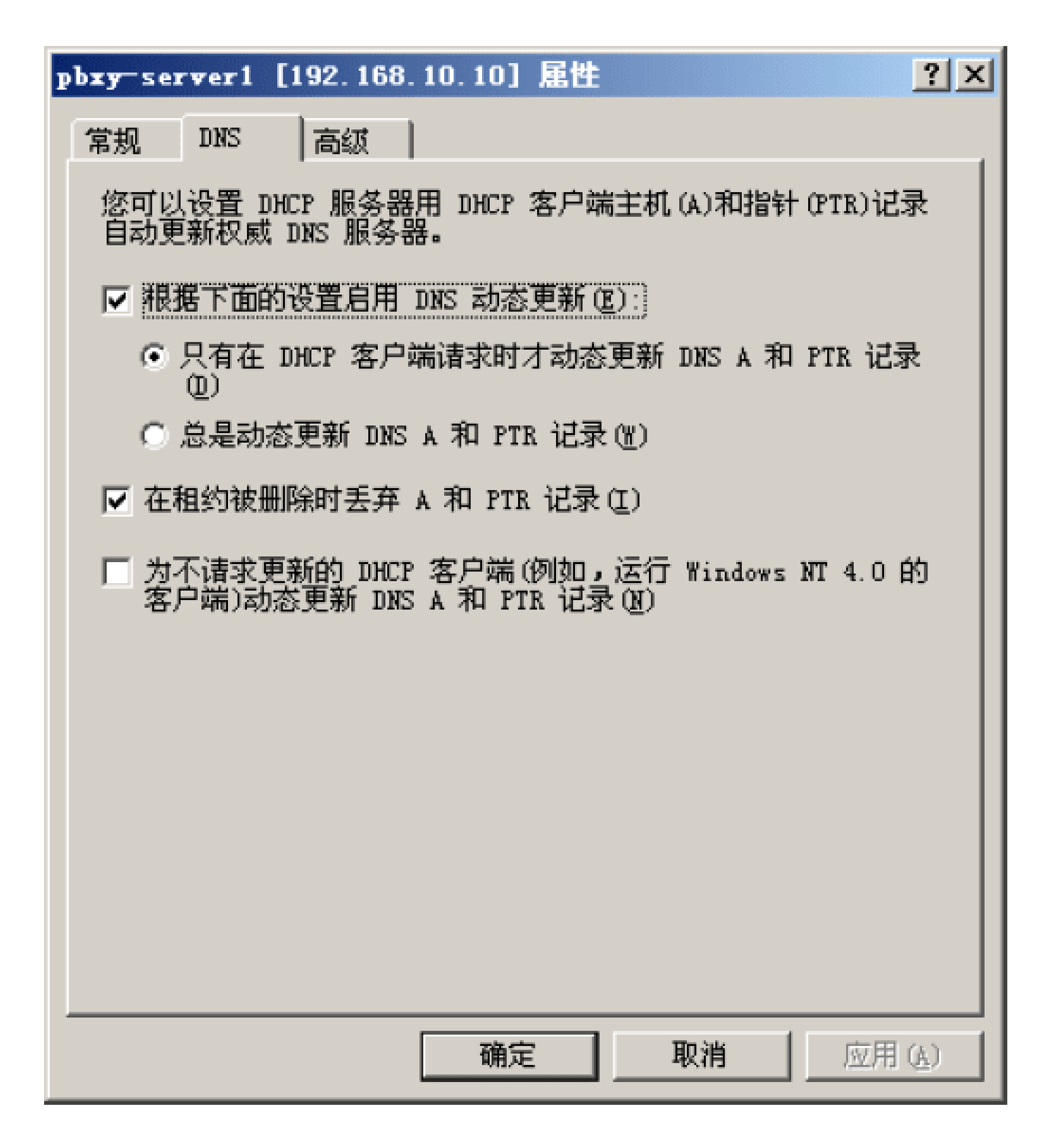


图 2-129　DNS 选项卡

(2)　在 DNS 选项卡中，如果用户希望 DNS 服务器的正向和反向查找能够在客户从

DHCP 服务器那里获得租约时自动更新，可以选中【根据下面的设置启用 DNS 动态更新】复选框。该功能包括两种可选方式：根据客户请求更新方式和总是动态更新 DNS 和 PTR 记录的方式。用户可以根据需要选中【只有在 DHCP 客户端请求时才动态更新 DNS A 和 PTR 记录】单选按钮或【总是动态更新 DNSA 和 PTR 记录】单选按钮中的一个，以便使用该方式启用 DNS 客户信息更新功能。

3) 设置【高级】选项卡

(1) 在选定的 DHCP 服务器的属性对话框中打开【高级】选项卡，如图 2-130 所示。

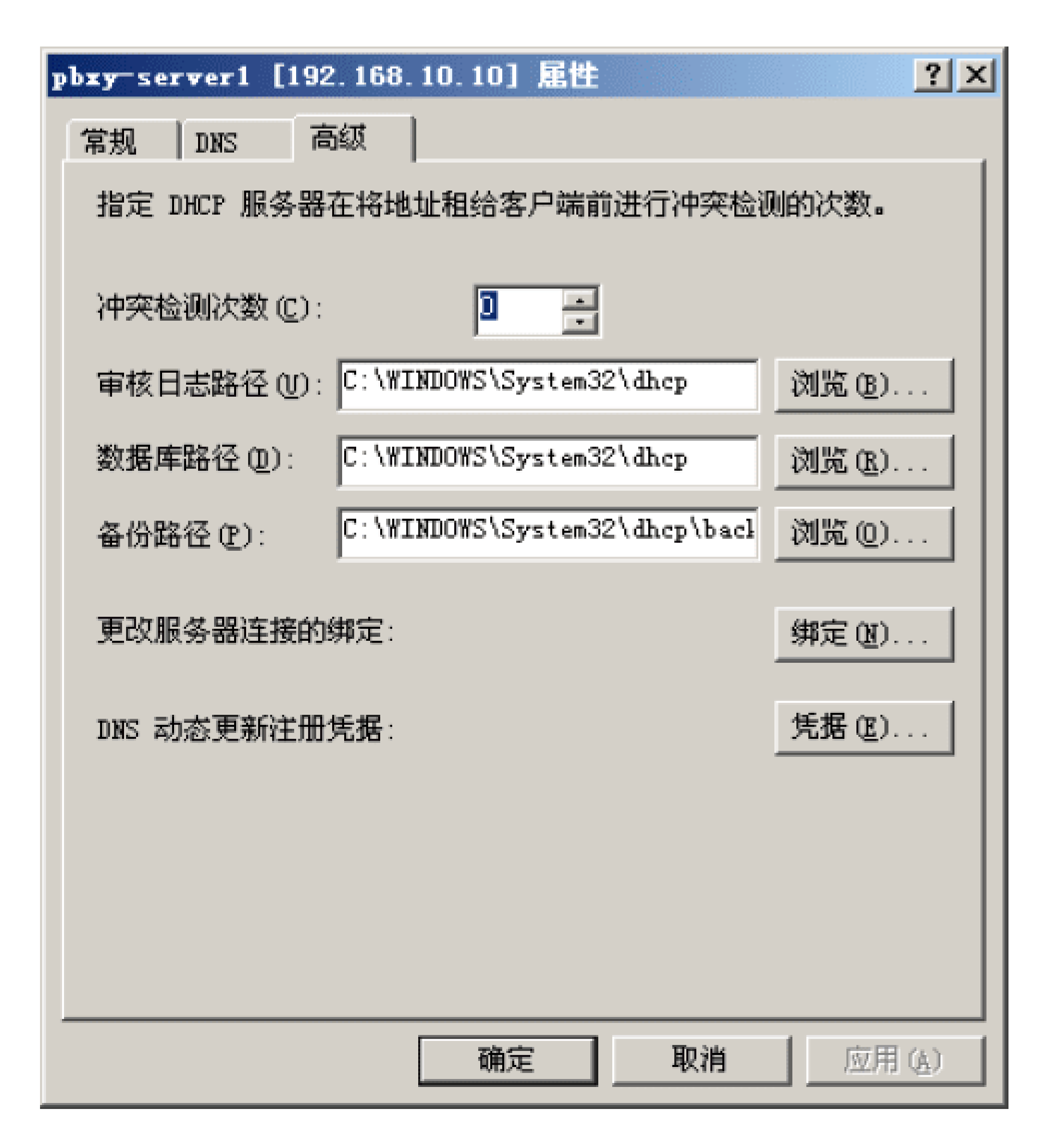


图 2-130 【高级】选项卡

(2) 在【高级】选项卡中，如果希望 DHCP 把 IP 地址租给客户之前，DHCP 服务器能够对将要分配的 IP 地址进行一定次数的冲突检测，可以通过【冲突检测次数】微调框来调整冲突检测的次数，以使 DHCP 按照指定的次数对 IP 地址进行检测。

(3) 如果用户希望更改 DHCP 中的数据库和审核文件在硬盘中的存储位置，可以分别在【审核日志路径】文本框和【数据库路径】文本框中输入指定的完整路径。另外，还可以单击【浏览】按钮，从打开的对话框中为审核日志或数据库选择一个存储路径。

(4) 如果需要更改 DHCP 服务器连接的绑定，可单击【绑定】按钮，系统将打开【绑定】对话框，如图 2-131 所示。在该对话框中，可以选择 DHCP 服务器为客户提供服务所支持的链接，单击【确定】按钮完成所有属性设置操作。

8. 停止、启动和重新启动 DHCP 服务

在 DHCP 服务器运行的过程中，需要 DHCP 服务的网络和 DHCP 服务器本身都有可能出现这样或那样的问题，此时，需要管理员及时对 DHCP 服务器进行断开、停止、暂停、重新开始等处理，以解决问题。

要停止、启动和重新启动 DHCP 服务，可参照下面的步骤。

(1) 打开 DHCP 控制台窗口，在控制台目录树中，单击要处理的 DHCP 服务器。

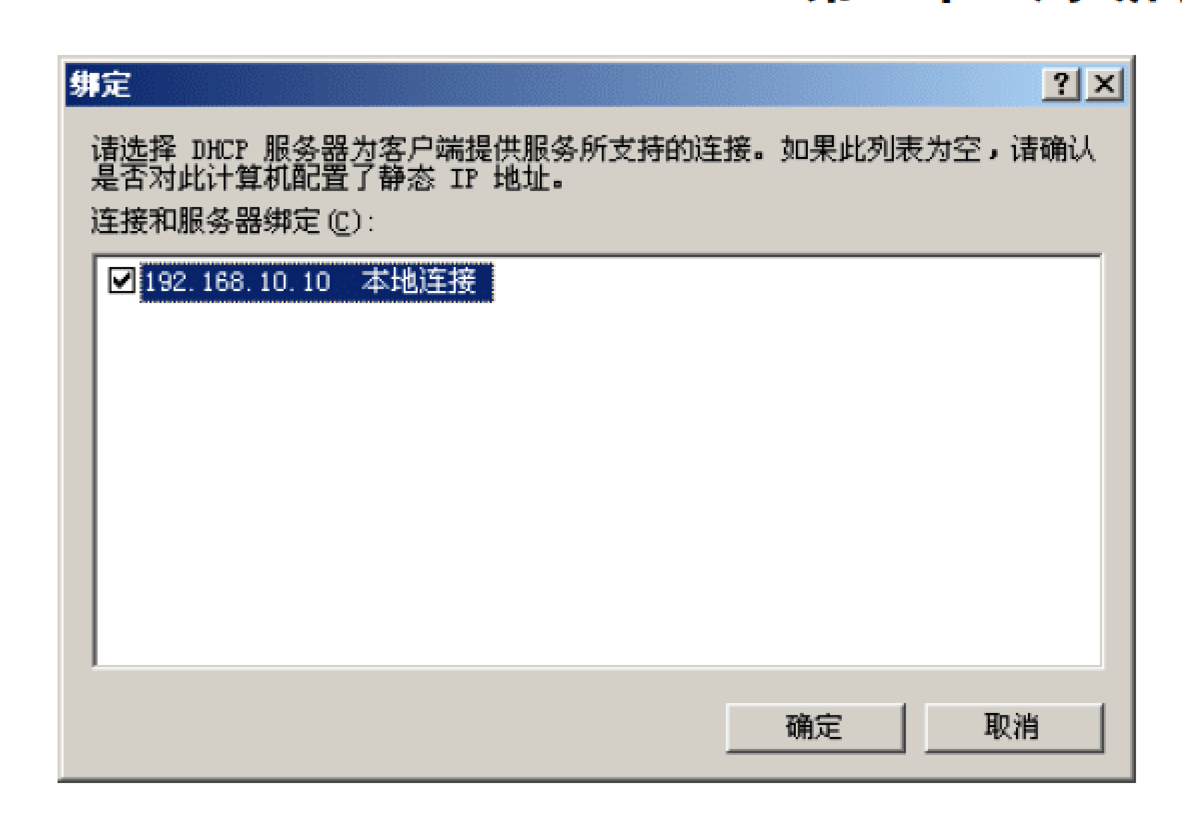


图 2-131　【绑定】对话框

(2) 若要对服务器进行停止和启动等操作，可选择【操作】|【所有任务】命令，然后选择下列命令之一。

- 要启动 DHCP 服务，可选择【开始】命令。
- 要停止 DHCP 服务，可选择【停止】命令。
- 要中断 DHCP 服务，可选择【暂停】命令。
- 重新开始 DHCP 服务，可选择【重新开始】命令。

(3) 在暂停 DHCP 服务后，将出现【恢复】命令，单击该命令可立即继续 WINS 服务。要断开服务器的连接，可选择【操作】菜单中的【删除】命令，出现信息提示框之后单击【是】按钮即可。

9. 查看作用域信息

在 DHCP 控制台目录中，每一个作用域下都有 4 个子项：地址池、地址租约、保留和作用域选项。通过它们，管理员可以查看到作用域的地址范围、地址排除范围、租约和保留情况以及选项设置等。

查看作用域信息的具体操作如下。

(1) 要查看作用域的地址范围和地址排除范围，可在 DHCP 控制台目录树中展开要操作的作用域，然后单击【地址池】子节点，在详细资料窗格中就会显示出相应的内容。

(2) 对于管理员，经常需要查看 DHCP 客户机的动态 IP 地址及其他租约情况，这是通过【地址租约】节点来完成的。在控制台目录树中单击【地址租约】子节点，在详细资料窗格中就会显示出网络中所有接受 DHCP 服务的计算机的租约情况，包括客户名称、IP 地址、租约最后日期、惟一 ID 号和类型等。

(3) 要查看地址保留选项，可在控制台目录树中单击【保留】节点，在详细资料窗格中就会显示出所有的自建保留，双击要查看的保留就可查看其内容。

(4) 右击作用域节点，从弹出的快捷菜单中选择【显示统计信息】命令，可打开该作用域的统计信息显示对话框。通过该对话框可查看该作用域的地址总数、已经使用的地址数和可用地址数，如图 2-132 所示。

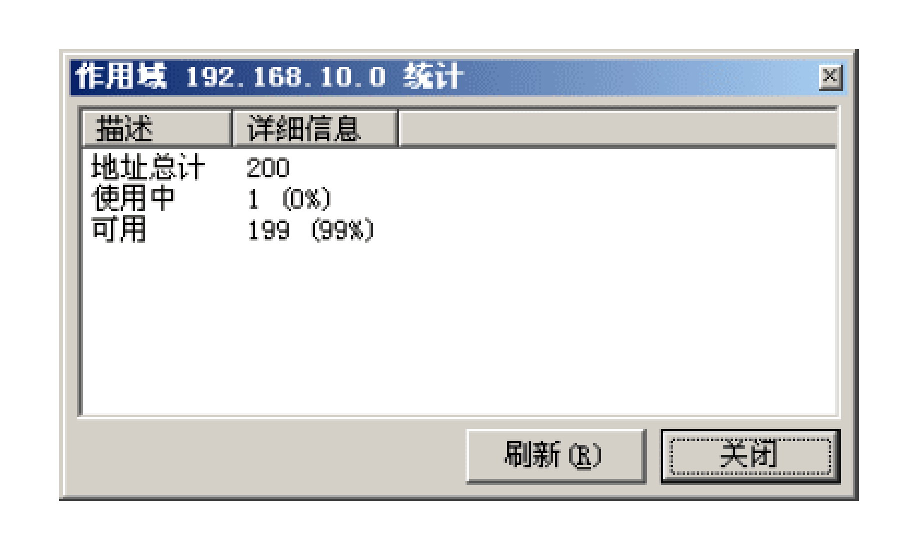


图 2-132　查看作用域地址使用情况

2.7.1.3 Red Flag Linux 下 DHCP 服务器的配置与管理

1. 启动 DHCP 配置工具

打开 DHCP 配置工具，可以采用以下方法启动 rfdhcp 工具。

- 在系统主菜单中选择【系统】|【控制面板】命令，打开【控制面板】窗口，在【网络服务配置】选项卡中，双击【DHCP 配置工具】。
- 在系统主菜单中选择【管理工具】|【DHCP 配置工具】命令。
- 在运行命令行或 shell 提示符下直接输入 rfdhcp。

2. 启动和停止 DHCP 服务

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的 DHCH 服务器；要启动 DHCP 服务，在菜单中选择【操作】|【所有任务】|【开始】命令；要停止 DHCP 服务，在菜单中选择【操作】|【所有任务】|【停止】命令；要重新启动 DHCP 服务，在菜单中选择【操作】|【所有任务】|【重新开始】命令。停止服务器之后，会出现【开始】选项并且可通过单击它再次恢复该服务。

也可以在命令行终端下，通过下列命令执行这些任务：

```
#/etc/rc.d/init.d/dhcpd/start
#/etc/rc.d/init.d/dhcpd/stop
#/etc/rc.d/init.d/dhcpd/restart
```

3. 查看 DHCP 服务器的属性

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的 DHCP 服务器。选择菜单中的【操作】|【属性】命令，打开【DHCP 属性】对话框，根据需要查看或修改服务器的属性。只有网络管理员才可以选择【授权此服务器为网络上的权威服务器】。如果不能确定自己是否具有网络管理员身份，请不要选择上述选项。

4. 授权 DHCP 服务器

DHCP 服务器在网络上正确配置和授权使用时，将提供有用且已计划好的管理服务。但是，当错误配置或未授权的 DHCP 服务器被引入网络时，可能会产生问题。例如，如果启动了未授权的 DHCP 服务器，它可能开始为客户机租用不正确的 IP 地址或者否认尝试更新当前地址租约的 DHCP 客户机。这些配置中的任何一个错误都可能导致启用 DHCP 的客户机产生更多的问题。例如，从未授权的服务器获取配置租约的客户机找不到有效的域控制器，致使客户机难以成功登录到网络。

为避免出现这些问题，在它们为客户提供服务之前，要在网络中验证服务器是否合法，这样就可避免由于在错误网络上运行带有不正确或正确配置的 DHCP 服务器而导致的大多数意外破坏。网络上运行的权威 DHCP 服务器将通知配置错误的 DHCP 客户机更新其配置。如果要指定一台 DHCP 服务器为权威服务器，在服务器的【属性】对话框中选中【授权此服务器为网络上的权威服务器】单选按钮。

5. 管理子网

管理子网是指对使用 DHCP 服务的子网进行的计算机管理性分组。管理员首先为每个

物理子网创建子网，然后使用该子网定义由客户机使用的参数。

1)　创建子网

(1) 打开 rfdhcp 工具，在主窗口左侧的控制台树中，单击相应的 DHCP 服务器、共享网络或群组。

(2) 在菜单中选择【操作】|【新建子网】命令，或者右击，从弹出的快捷菜单中选择【新建子网】命令，也可以单击工具栏中的【新建子网】按钮，弹出【新建子网向导】对话框。

(3) 在欢迎界面中，单击【下一步】按钮继续，出现【子网 ID 与掩码】设置界面。在【网络 ID】文本框中输入新建子网的网络标识，在下面的【长度】和【子网掩码】文本框中会自动出现对应的数据。可以根据需要修改。

(4) 单击【下一步】按钮，规划将发放的 IP 地址范围。

(5) 在此可以通过输入【起始 IP 地址】和【结束 IP 地址】来确定多个连续的 IP 地址范围；如果要添加一个单独的地址，则只在【起始 IP 地址】中输入数值即可。每设置一个 IP 地址范围后，单击【添加】按钮将其加入地址范围列表中。

(6) 单击【下一步】按钮，设置客户端得到 IP 地址的租约时间长度。一般而言，对于一个变动性较高的局域网，就要设置较短的租约期限；而对于一个主要包含台式计算机，位置固定的网络来说，就应该设置较长的租约期限。

(7) 单击【下一步】按钮，出现配置选项界面，这时已经设置了一个子网的基本配置。向导提示配置常用的 DHCP 选项以使用新建的子网。

(8) 如果不打算设置这些选项，可以选中【否，我想稍后配置这些选项】单选按钮。这些选项可以在【子网选项】中进行设置。

(9) 依照默认的选中【是，我想现在配置这些选项】单选按钮，单击【下一步】按钮继续。

(10) 输入为子网分配的路由器或默认网关的 IP 地址，然后单击【添加】按钮，也可以输入服务器名称。

(11) 单击【解析】按钮让系统自动寻找其 IP 地址。如果没有预设的路由器或网关，则不必输入任何数据。

(12) 单击【下一步】按钮继续，进入域名称和 DNS 服务器设置界面。

(13) 输入子网上的计算机进行 DNS 名称解析时使用的父域；如果有 DNS 服务器，输入其名称或 IP 地址后单击【添加】按钮，也可以输入服务器的名称后，单击【解析】按钮让系统自动寻找其 IP 地址。

(14) 单击【下一步】按钮，进行 WINS 服务器的相关设置，完成此步骤后，单击【下一步】按钮会出现完成新建子网向导界面。

(15) 单击【完成】按钮，重新启动 dhcpd 服务后，客户端就可以使用这个子网中的地址了。

2)　删除子网

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的子网。选择菜单中的【操作】|【删除】命令。出现提示时，请确认是否删除该子网。无法删除共享网络中惟一的子网。

3) 向子网中加入地址范围

在 rfdhcp 配置工具主窗口左侧的控制台树中，展开相应的子网，选择【地址池】选项。选择菜单中的【操作】|【新建地址范围】命令，也可以右击，并选择弹出快捷菜单中的【新建地址范围】命令。在打开的【新建地址范围】对话框中，输入要向该子网中添加的 IP 地址范围的【起始 IP 地址】和【结束 IP 地址】。如果只要添加一个单独的地址，则只输入【起始 IP 地址】即可。如果希望服务器将这个范围内的地址动态分配给 BOOTP 客户，请选中【允许 BOOTP 客户】单选按钮。单击【添加】按钮，新增的地址范围将显示在主窗口右侧的地址池列表中。

4) 更改或查看子网属性

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。选择菜单中的【操作】|【属性】命令，或右击，并选择弹出快捷菜单中的【属性】命令。打开【子网属性】对话框，可以根据需要查看或修改子网的属性。

5) 查看客户机租约信息

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应子网的【地址租约】项。在窗口右侧的详细信息列表中，可以查看客户机的租约信息。

6. 管理共享网络

可以通过 DHCP 配置工具创建和管理 DHCP 服务器使用共享网络将多个子网组合为单个管理实体。

1) 创建共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的 DHCP 服务器或群组；选择菜单中的【操作】|【新建共享网络】命令，也可以右击，并在弹出的快捷菜单中选择【新建共享网络】命令，该菜单项只有在至少已经在服务器或群组中创建了一个子网，而且它目前不是共享网络或其他群组的一部分时才显示；在【新建共享网络向导】中，按提示信息完成操作。

2) 删除共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的共享网络。选择菜单中的【操作】|【删除】命令，也可以右击，并在弹出的快捷菜单中选择【删除】命令。出现提示时，确认是否删除共享网络。删除共享网络会删除所有包含在其中的成员子网、主机、群组。如果想保留某个成员，在删除共享网络之前先将它移到服务器或其他共享网络中即可。

3) 将子网添加到共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。用鼠标将子网拖曳到希望加入的共享网络中，出现提示时，单击【是】按钮即可完成子网的移动。

7. 管理主机

使用主机保留地址，可以将特定的 IP 地址分配给特定的 DHCP 客户机使用。此外，也可以通过主机将一组固定的设置参数提供给指定的某些网络客户机。

1) 添加主机

(1) 在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应子网的【保留】项。

(2) 选择菜单中的【操作】|【新建主机】命令，也可以在右键快捷菜单中选择【新建

主机】命令。

(3) 在【新建主机】对话框中，输入要保留的客户机名称与 IP 地址，以及客户机的 MAC 地址。

(4) 填完后单击【添加】按钮，如果不再增加其他保留地址，则单击【关闭】按钮结束。相应的主机将添加到该子网中。关于保留主机，有以下几点说明请注意：可以在服务器、共享网络、群组和子网保留中添加主机，可以明确指定主机的 IP 地址，也可以不添加任何地址。由 DHCP 服务器动态为客户机分配地址；主机硬件一般是在相应网络连接的 DHCP 客户机媒体访问控制(MAC)地址的基础上确认的；除以太网外，DHCP 服务器也支持令牌环硬件类型，但暂不支持 FDDI 硬件；DHCP 服务器通过客户发送的惟一客户机识别码来确认客户，这个识别码由常规选项【061 惟一客户机识别码】来确定。如果这个识别码没有被定义，则需要通过对方的媒体访问控制(MAC)地址来识别主机客户。

2) 删除主机

打开 rfdhcp 工具，在主窗口左侧的控制台树中，选择相应的主机。选择菜单中的【操作】|【删除】命令，也可以右击，并在弹出的快捷菜单中选择【删除】命令。出现提示时，请确认是否删除该主机。

3) 更改或查看主机属性

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的主机。选择菜单中的【操作】|【属性】命令，也可以右击，并在弹出的快捷菜单中选择【属性】命令。打开主机属性对话框，可以根据需要查看或修改主机的属性。

8. 管理群组

使用群组，可以将多个子网、共享网络、主机组合为单个管理实体。

对于群组成员没有定义的参数设置，DHCP 服务器会自动应用成员所属群组中的参数定义值。

1) 创建群组

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的 DHCP 服务器、共享网络、子网或者群组。选择菜单中的【操作】|【新建群组】命令，也可以右击，并在弹出的快捷菜单中选择【新建群组】命令。在打开的【新建群组向导】对话框中，按提示信息完成操作。

2) 删除群组

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的群组。

选择菜单中的【操作】|【删除】命令，也可以右击，并在弹出的快捷菜单中选择【删除】命令。出现提示时，请确认是否删除该群组。

3) 添加成员到群组中

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择希望加入群组的成员节点，群组成员可以是子网、主机、共享网络或者其他的群组。用鼠标将目标成员拖拽到目的群组中，出现提示时，单击【是】按钮即可移动该节点。

9. 设置选项

在为客户机设置了基本的 TCP/IP 配置(如 IP 地址、子网掩码和默认网关)之后，大多数

客户机同时还需要 DHCP 服务器通过 DHCP 选项提供其他信息。

在子网、主机、共享网络以及群组中没有指派的选项将自动套用其父系节点中指派的值。

(1) 在 rfdhcp 配置工具主窗口左侧的控制台树中，展开想要配置其选项的服务器、子网、共享网络或群组，选择“xxx 选项”(xxx 代表所选的节点名称)。选择菜单中的【操作】|【配置选项】命令，也可以右击，并在弹出的快捷菜单中选择【配置选项】命令。打开选项设置对话框，可以根据需要查看或修改对应节点的选项。

(2) 在【可用选项】列表中，选中希望配置的对应选项；选中该选项前的复选框以激活窗口下面的【数据输入】文本框，输入该选项所需的必要信息。

(3) 对于任何其他希望配置的选项，请重复以上的步骤，最后单击【确定】按钮。

10. 使用 rfdhcp 的文件编辑器

为了使用户能够全面地配置 DHCP 服务器支持的全部功能，rfdhcp 配置工具提供了一个文件编辑器。用户可以通过这个编辑器直接对 DHCP 配置文件进行手工修改。配置工具也可以检查配置文件的语法错误。语法检查结果会显示在输出消息窗口中。

(1) 默认情况下，主窗口中不显示配置文件编辑区。在菜单中选择【查看】|【编辑器】命令，显示配置文件编辑窗口。

(2) 在编辑器窗口中对配置文件进行手工修改后，单击工具栏上的【保存】按钮，保存文件。然后查看输出信息中的语法检查结果。如果出现语法错误，请根据提示进行修改。修改完成后，重复上面的步骤。

注意：在开始手工修改配置文件后，不要在存储文件之前使用配置工具提供的其他配置功能，否则所作的修改将会被覆盖；配置文件修改并存储后，必须重新启动 DHCP 服务器才能使修改生效；输出信息中所显示的蓝色信息属于警告，红色信息属于错误；租约数据库文件不能用配置工具修改。修改租约文件可能会导致 DHCP 服务器掌握的租约信息不正确，因此在正常情况下，不应对租约文件做任何修改。可以使用如下的命令来指定配置文件和租约文件的路径：rfdhcp - cf < configuration file = -lf < lease file >。一般情况下，请不要指定自己的租约文件，因为租约信息不正确会影响 DHCP 服务器的正常工作。

2.7.1.4 Linux 下 DHCP 服务器的配置与管理

虽然在 Windows 2000 Server、Windows Server 2003 和 Red Flag Linux 环境下都可以用图形化界面来配置和管理 DHCP 服务器，读者还有必要了解在 Linux 下 DHCP 服务器的配置。

1. DHCP 服务器软件的安装

在 Linux 下几乎都是采用 Paul Vixie/ISC DHCPd 来实现 DHCP 服务器端功能。用户可以访问 http://www.isc.org/isc 获得最新消息。

目前大多数 Linux 发布盘中都包含这个软件，并以 RPM 形式提供。用户只要以 root 身份登录，简单地用 RPM 安装就可以了。其命令格式为：

```
# rpm -ivh dhcpd-1.3.17pl5.i386.rpm    //1.3.17pl5 为 DHCP 版本号
```

2. 增加主机路由

为了使 DHCP 服务器能为正确 Windows 的 DHCP 客户机服务，需要创建一个到地址 255.255.255.255 的路由，把这条路由命令加到/etc/rc.d/rc.local，使得每次机器启动后自动运行。其命令格式为：

```
#route add -host 255.255.255.255 dev eth0
```

在一些旧版 Linux 核心的系统中可能会报告错误消息：

```
255.255.255.255: Unkown host
```

可以试着将下面的条目加到/etc/hosts 文件中：

```
255.255.255.255 dhcphost
```

再用下面的命令：

```
#route add -host dhcphost dev eth0
```

3. 修改配置文件

DHCP 服务默认的配置文件是/etc/dhcpd.conf，这是一个文本文件，DHCP 服务里有一个语法分析器，能对这个文件进行语法分析，获得配置参数。dhcpd.conf 格式是递归下降的，关键字大小写敏感，可以有注释，注释以“#”开头，一直到该行结束(为了显示清晰，下例中把注释移到行尾，在实际配置时是不允许的)。这里给出一个简单的 dhcpd.conf 的例子，所服务的网络为 C 类保留网络 192.168.1.0。

```
#dhcpd.conf 配置实例
subnet 192.168.1.0 netmask 255.255.255.0 {      # 子网声明和掩码
range 192.168.1.10 192.168.1.100;               # 范围
range 192.168.1.150 192.168.1.200;              # 范围
#全局参数设置
default-lease-time 28800;                       # 默认租约时间
max-lease-time 43200;                           # 最大租约时间
option subnet-mask 255.255.255.0;               # 子网掩码选项
option broadcast-address 192.168.1.255;         # 广播地址
option routers 192.168.1.1;                     # 路由器地址
option domain-name-servers 192.168.1.1;         # DNS 地址
option domain-name "netreslab.org";             # 域名
}
```

这段配置文件将允许 DHCP 服务器分配两段地址范围给 DHCP 客户，192.168.1.10～192.168.1.100 和 192.168.1.150～192.168.1.200；如果 DHCP 客户在申请租约时不请求一个特定租约失效时间，则以 default-lease-time(28800 秒)为租约时间，如果有请求一个特定的租约失效时间，则采用 max-lease-time(432000 秒)。

服务器发送下面的参数给 DHCP 客户机：子网掩码是 255.255.255.0 ，广播地址是 192.168.1.255，默认网关是 192.168.1.1，DNS 是 192.168.1.1。

如果要为一台叫做 hotdog 的机器指定固定的 IP 地址，可以在 dhcpd.conf 文件中增

加一条：

```
host hotdog {                              # 为 hotdog 指定固定的 IP 地址
hardware ethernet 08:00:00:4c:58:23;       # hotdog 上网卡的硬件地址
fixed-address 192.168.1.210;               # 固定 IP
}
```

4. dhcpd.leases 文件

dhcpd.leases 是 DHCP 客户租约的数据库文件，默认目录为/var/state/dhcp/，文件包含租约声明。每次一个租约被获取、更新或释放，它的新值就被记录到文件的末尾。在 dhcpd 第一次安装后，并不会生成这个文件。但 dhcpd 的运行需要这个文件，所以可以建立一个空的文件：

```
#touch /var/state/dhcp/dhcpd.leases
```

dhcpd 记录这个文件的格式是：

```
lease ip-address { statements... }
```

每个记录包含一个提供给客户的 IP 地址，在花括号里的语句包含一些租约信息。具体的租约信息因客户发出不同的 DHCP 请求而稍有差别。

如果我们启动一台 Windows 98 机器，可以在 Windows 98 的网络配置的 TCP/IP 选项中指定自动获得 IP 地址，也就是启用 Windows 98 中的 DHCP 客户程序，这台机器的主机名为 ONE。在 Windows 98 机器获得租约后，dhcpd 会在 dhcpd.leases 中创建一条记录：

```
lease 192.168.1.154 {
starts 1 2000/05/15 13:36:42;
ends 1 2000/05/15 21:36:42;
hardware ethernet 00:00:21:4e:3f:58;
uid 01:00:00:21:4e:3f:58;
client-hostname one;
}
```

要注意的是，dhcpd.leases 的时间记录采用 GMT 时间，而不是本地时区的时间。要查看本机的 GMT 时间可以用“date -u”命令。

5. 运行 DHCP 服务

用户可以使用 dhcpd 守护程序来启动、重新启动、停止 DHCP 服务。

启动 DHCP 服务的命令是：

```
/etc/rc.d/init.d/dhcpd start.
```

这样启动后，dhcpd 是启动在 eth0 上。如果 dhcpd 上的服务器还有另外一块网卡 eth1，想在 eth1 上启动 DHCP 服务，命令是：

```
#/usr/sbin/dhcpd eth1
```

如果在修改配置文件 dhcpd.conf 后，希望立即生效，可重新启动 DHCP 服务，其命令是：

```
#/etc/rc.d/init.d/dhcpd restart
```

如果希望暂时停止 DHCP 服务，其命令是：

```
#/etc/rc.d/init.d/dhcpd stop
```

设定 DHCP 服务在计算机启动时自动启动或不启动，可以使用 ntsysv 命令将它加到引导程序中。也可以通过 chkconfig 命令来设定，该命令格式是：

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如，我们希望在运行级别 3、5 启动计算机时启动 DHCP 服务，则命令为：

```
#chkconfig --level 35 dhcpd on
```

再如，我们希望在运行级别 2 启动计算机时不启动 DHCP 服务，则命令为：

```
#chkconfig --level 2 dhcpd off
```

如果希望在任何运行级别下启动时都不启动 DHCP 服务，只要不设定“[--level <运行级>]”就可以了，即：

```
#chkconfig dhcpd on
#chkconfig dhcpd off
```

6. dhcpd.conf 详解

1) dhcpd.conf 概述

前面说过，dhcpd.conf 是个递归下降格式的配置文件，有点像 C 语言的源程序风格，由参数和声明两大类语句构成。参数类语句主要告诉 DHCPd 网络参数，如租约的时间、网关、DNS 等；而声明语句则是描述网络的拓扑，用来表明网络上的客户和要提供给客户的 IP 地址以及提供一个参数组给一组声明等。

描述网络拓扑的声明语句有 shared-network 和 subnet。如果要给一个子网中的客户动态指定 IP 地址，那么在 subnet 声明中必须有一个 range 声明，来说明地址范围。如果要给 DHCP 客户静态指定 IP 地址，那么每个这样的客户都要有一个 host 声明。对于每个要提供服务的与 DHCP 服务器连接的子网，都要有一个 subnet 声明，即使这是个没有 IP 地址要动态分配的子网也需要有。

2) 语句参考

因为 DHCPd 的语句很多，不可能一一列出，这里给出最常用和最重要的语句。

(1) 声明类语句

① share-network 语句

语法：

```
shared-network name {
[ 参数 ]
[ 声明 ]
}
```

说明：share-network 用于告知 DHCP 服务器某些 IP 子网其实是共享同一个物理网络。任何一个在共享物理网络中的子网都必须声明在 share-network 语句里。当属于其子网中的客户启动时，将获得在 share-network 语句里指定参数权限，除非这些参数被 subnet 或 host

中的参数覆盖。用 share-network 是一种权宜之计，例如，某公司用 B 类网络 145.252，公司里的部门 A 被划在子网 145.252.1.0 里，子网掩码为 255.255.255.0，这里子网号为 8 位，主机号也为 8 位，但如果部门 A 急速增长，超过了 254 个节点，而物理网络还来不及增加，就要在原来这个物理网络上加两个 8 位掩码的子网，而这两个子网其实是在同一个物理网络上。share-network 语句形式如下：

```
shared-network share1 {
subnet 145.252.1.0 netmask 255.255.255.0 {
range 145.252.1.10 145.252.1.253;
}
subnet 145.252.2.0 netmask 255.255.255.0 {
range 145.252.2.10 145.252.1.253;
}
```

这里的 share1 是个共享网络名。

② subnet 语句

语法：

```
subnet subnet-number netmask netmask {
[ 参数 ]
[ 声明 ]
}
```

说明：subnet 语句用于提供足够的信息来阐明一个 IP 地址是否属于该子网。也可以提供指定的子网参数和指明那些属于该子网的 IP 地址可以动态分配给客户，这些 IP 地址必须在 range 声明中指定。subnet-number 可以是个 IP 地址或能被解析到这个子网的子网号的域名。netmask 可以是个 IP 地址或能被解析到这个子网的掩码的域名。

③ range 语句

语法：

```
range [ dynamic-bootp ] low-address [ high-address];
```

说明：对于任何一个有动态分配 IP 地址的 subnet 语句，至少要有一个 range 语句，用来指明要分配的 IP 地址的范围。如果只指定一个要分配的 IP 地址，那么高地址部分可以省略。

④ host 语句

语法：

```
host hostname {
[ 参数 ]
[ 声明 ]
}
```

说明：host 语句的作用是为特定的客户机提供网络信息。

⑤ group 语句

语法：

```
group {
[ 参数 ]
```

```
[ 声明 ]
}
```

说明：group 语句的作用是给一组声明提供参数。

⑥　allow 和 deny 语句

allow 和 deny 语句用来控制 dhcpd 对客户的请求。

```
allow unknown-clients;
deny unknown-clients;
```

allow unknown-clients 允许 dhcpd 可以动态分配 IP 给未知的客户，而 deny unknown-clients 则不允许。默认为允许。

⑦　bootp 关键字

```
allow bootp;
deny bootp;
```

bootp 关键字指明 dhcpd 是否响应 bootp 查询。默认为允许。

(2)　参数类语句

①　default-lease-time 语句

语法：

```
default-lease-time time;
```

说明：该语句指定默认租约时间，这里的 time 是以秒为单位的。它用来指定 DHCP 客户机在租约 IP 地址后什么时间需要向 DHCP 服务器重新申请 IP 地址租约。

②　max-lease-time 语句

语法：

```
max-lease-time time;
```

说明：该语句指定最大的租约时间。如果 DHCP 在请求租约时间时有发出特定的租约失效时间的请求，则用最大租约时间。

③　hardware 语句

语法：

```
hardware hardware-type hardware-address;
```

说明：该语句用于指明物理硬件接口类型和硬件地址。硬件地址由 6 个 8 位组构成，每个 8 位组以“:”隔开，如 00:00:E8:1B:54:97。

④　server-name 语句

语法：

```
server-name name;
```

说明：该语句用于告知客户服务器的名称。

⑤　fixed-address 语句

语法：

```
fixed-address address [, address ... ];
```

说明：fixed-address 语句用于指定一个或多个 IP 地址给一个 DHCP 客户。只能出现在 host 声明中。

(3) 选项类语句

选项类语句以 option 开头，后面跟一个选项名，选项名后是选项数据，选项非常多。这里列出一些常用的选项供参考。

① option subnet-mask < subnet-netmask>;

该选项用于指明子网掩码。

② option routers ip-address[, ip-address];

该选项用于指明在子网内的默认网关(即路由器)的地址，可以有多个。

③ option time-servers ip-address[, ip-address...];

该选项用于指明时间服务器的地址。

④ option domain-name-servers ip-address[, ip-address...];

该选项用于指明 DNS 的地址。

⑤ option host-name string;

该选项用于给客户指定主机名，string 为字符串。

⑥ option domain-name string;

该选项用于指明域名。

⑦ option interface-mtu mtu;

该选项用于指明网络界面的 mtu，这里 mtu 为正整数。

例如，option interface-mtu 1500;。

⑧ option broadcast-address ip-address;

该选项用于指定广播地址。

2.7.2 典型例题分析

例 1 阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 5 月下午试题一)

【说明】

某局域网的 IP 地址为 61.100.13.0/24，采用 DHCP 服务器(DHCPServer)自动分配 IP 地址，网络结构如图 2-133 所示。

【问题 1】(每空 1 分，共 6 分)

PCI 首次启动时，DHCP 工作流程为：寻找 DHCP 服务器、提供 IP 租用、接受 IP 租约及租约确认等四步，如图 2-134 所示。

为图 2-134 中(1)～(4)处选择正确的报文。

(1)～(4)备选答案：

A. Dhcpdiscover　　B. Dhcpoffer

C. Dhcprequest　　D. Dhcpack

客户端所发出的 Dhcpdiscover 报文中，源 IP 地址为 (5) ，目的 IP 地址为 (6) 。

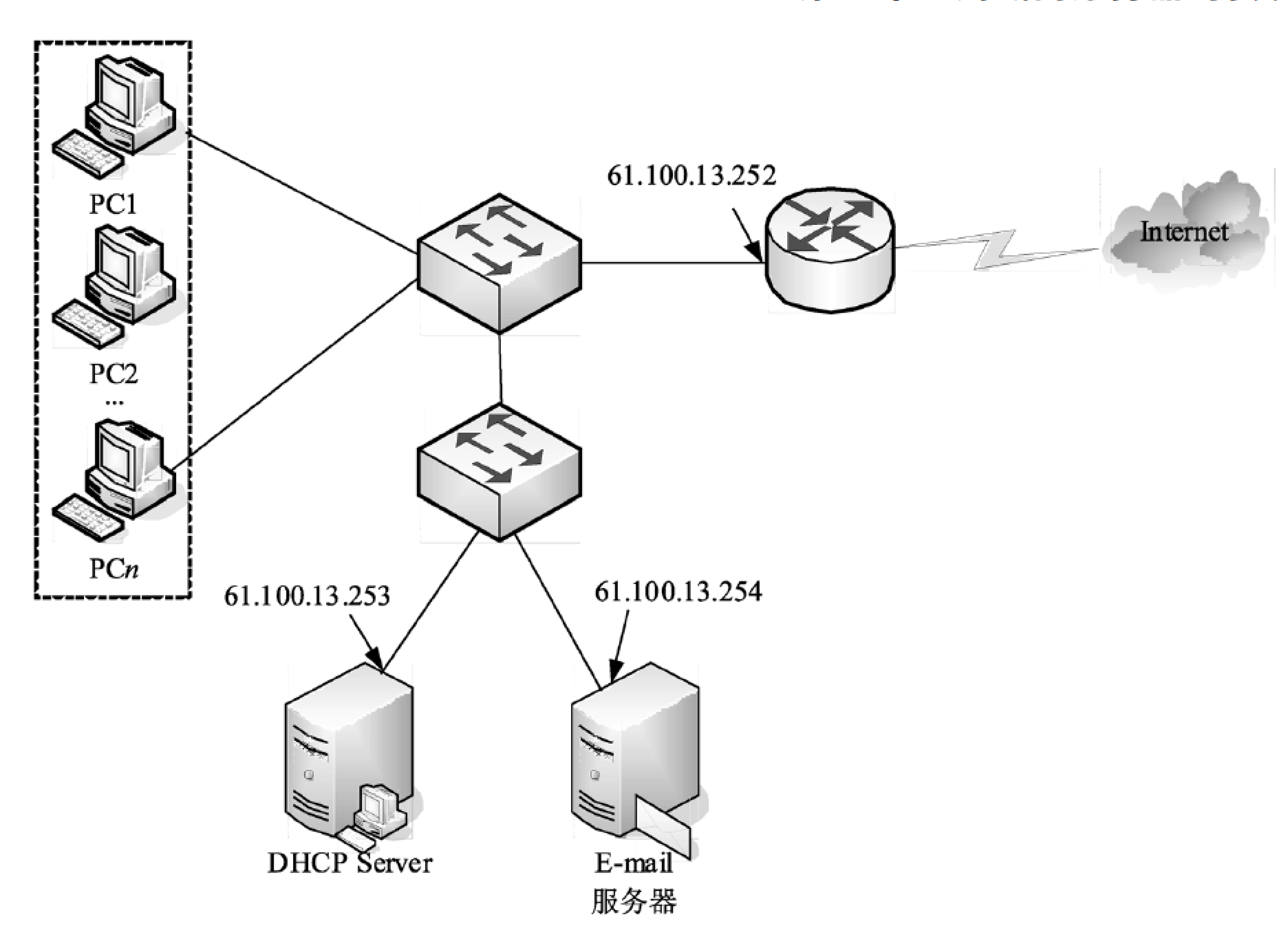


图 2-133　某局域网网络结构

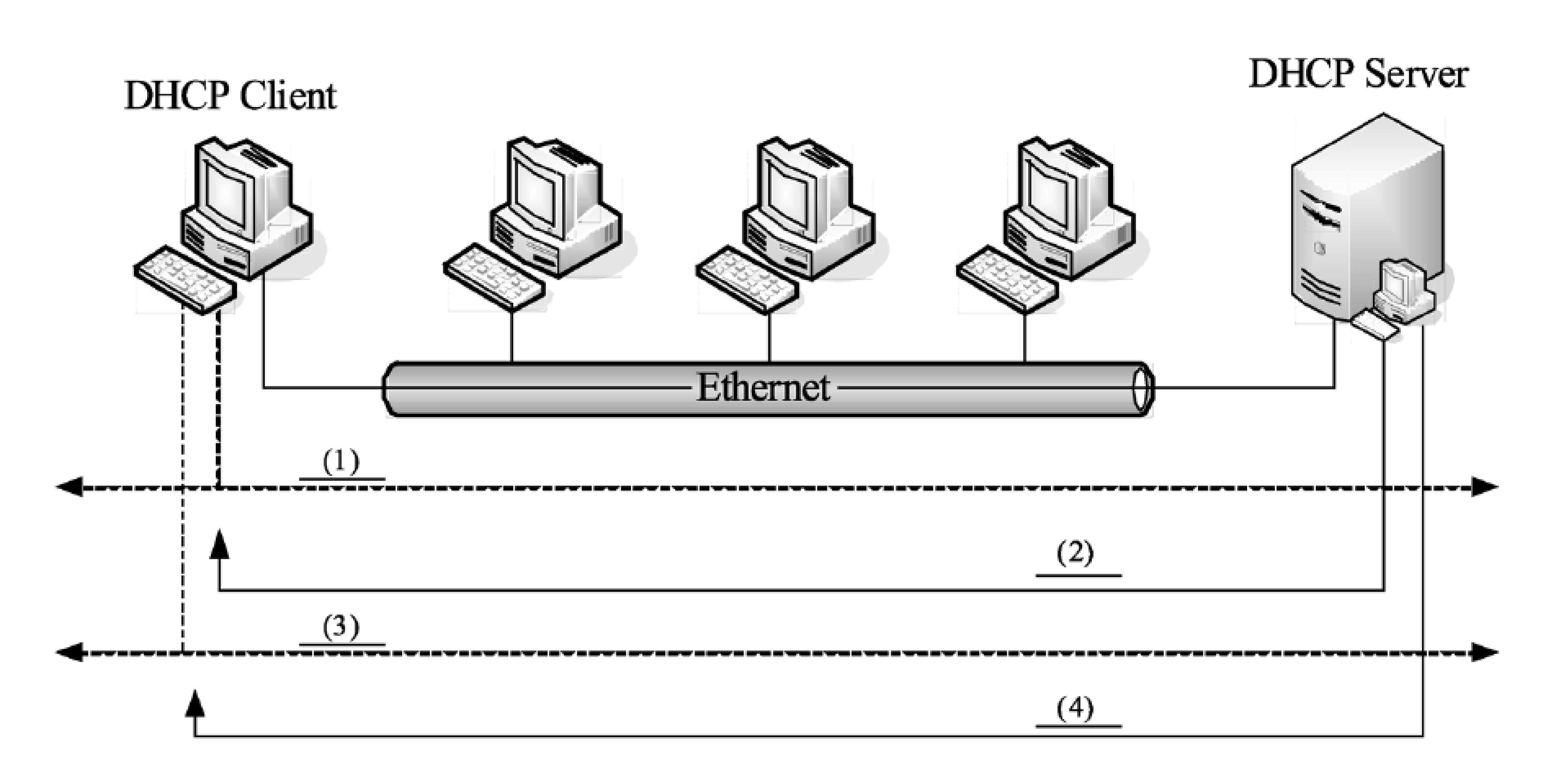


图 2-134　DHCP 工作流程示意

【问题 2】(每空 2 分，共 4 分)

图 2-135 是 DHCPServer 中服务器配置时分配 IP 地址的范围窗口。

为图 2-135 中的 DHCPServer 配置属性参数。

起始 IP 地址：　(7)

结束 IP 地址：　(8)

【问题 3】(1 分)

如图 2-136 所示的 PCl 的 Internet 协议属性参数应如何设置？

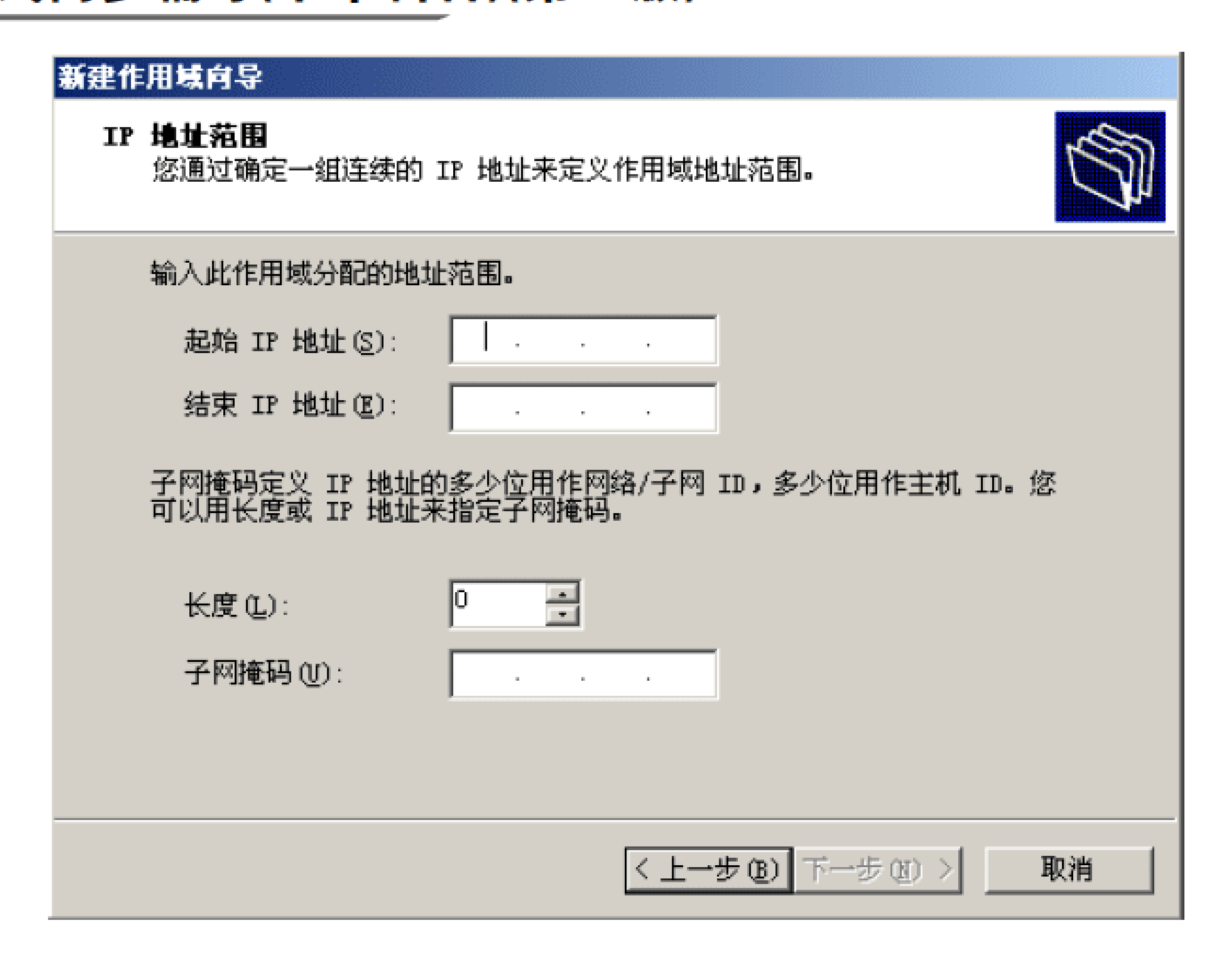


图 2-135 【IP 地址范围】对话框

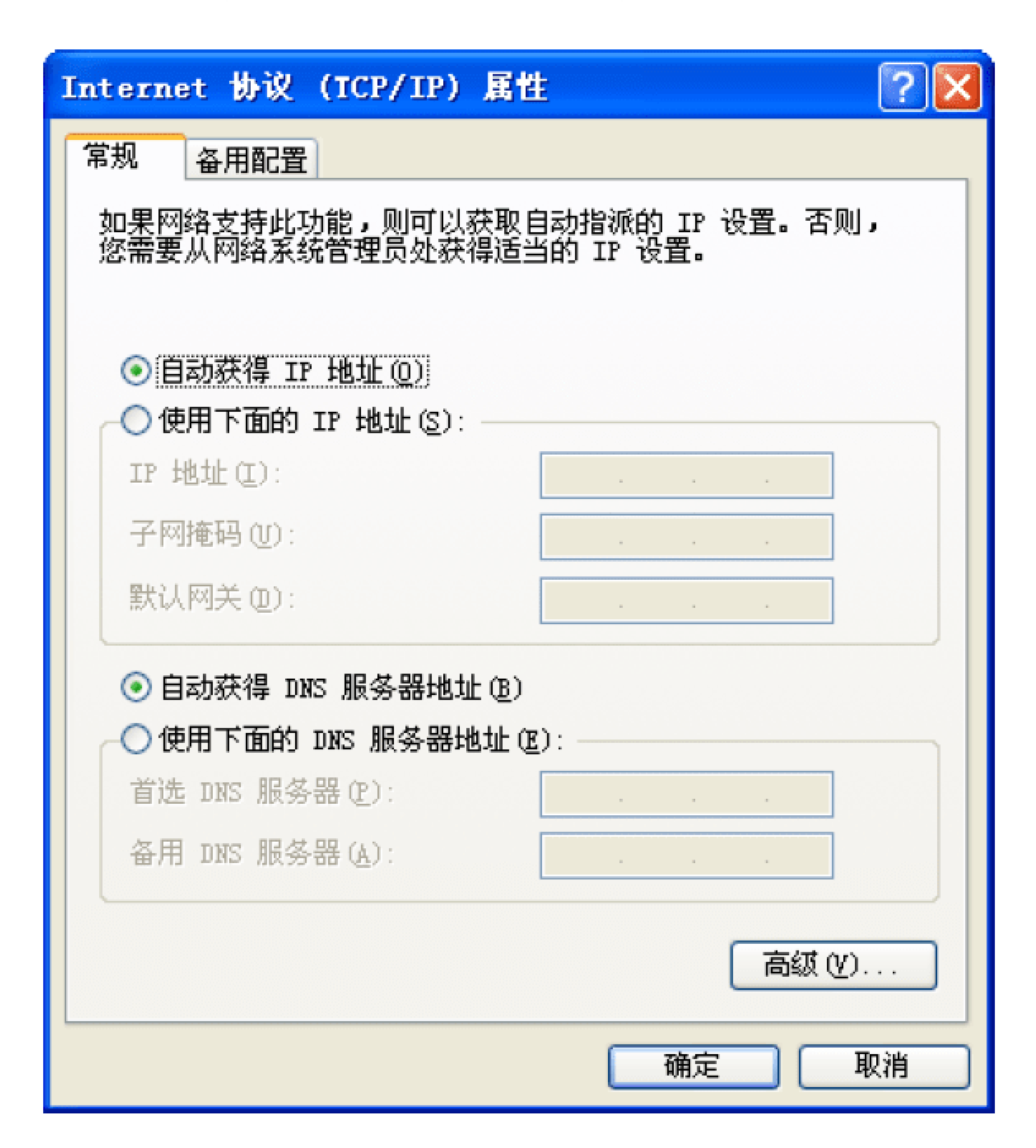


图 2-136 【Internet 协议(TCP/IP)属性】对话框

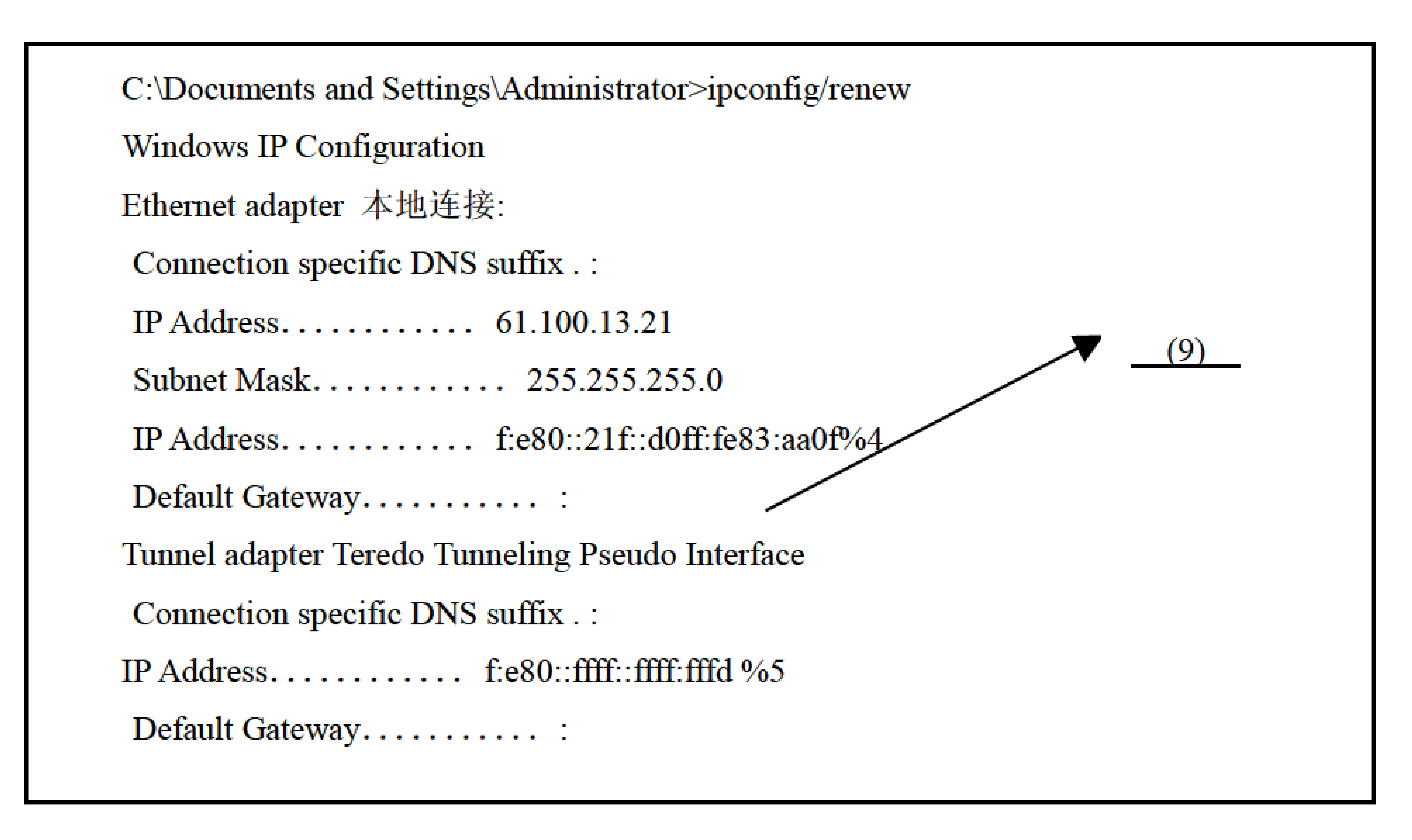
【问题 4】(每空 2 分，共 4 分)

图 2-137 是 PCI 采用 ipconfig/renew 重新租用 IP 地址的命令窗口，在__(9)__处填入正确的 IP 地址。

图 2-137 表明，PCI__(10)__。

A. 仅分配了 IPv4 地址　　B. 仅分配了 IPv6 地址

C. 既分配了 IPv4 地址，又分配了 IPv6 地址



```
C:\Documents and Settings\Administrator>ipconfig/renew
Windows IP Configuration
Ethernet adapter  本地连接:
 Connection specific DNS suffix . :
 IP Address. . . . . . . . . . . .  61.100.13.21
 Subnet Mask. . . . . . . . . . . .  255.255.255.0
 IP Address. . . . . . . . . . . .  f:e80::21f::d0ff:fe83:aa0f%4
 Default Gateway. . . . . . . . . .  :
Tunnel adapter Teredo Tunneling Pseudo Interface
 Connection specific DNS suffix . :
IP Address. . . . . . . . . . . .  f:e80::ffff::ffff:fffd %5
 Default Gateway. . . . . . . . . .  :
```


图 2-137　执行 ipconfig/renew 命令系统的返回信息

分析：

本题考查 Windows 操作系统配置中 DHCP 服务器的配置情况。

【问题 1】

第一次登录时，DHCP 工作流程为：寻找 DHCP 服务器、提供 IP 租用、接受 IP 租约及租约确认 4 步。

① 寻找 Server。当 DHCP 客户端第一次登录网络时，客户发现本机上没有任何 IP 资料设定，它会向网络发出一个 Dhcpdiscover 包。由于客户端还不知道自己属于哪一个网络，所以包的源地址设置为 0.0.0.0，而目的地址则设置为 255.255.255.255，然后再附上 Dhcpdiscover 的信息，向网络进行广播。

② 提供 IP 租用地址。当 DHCP 服务器监听到客户端发出的 Dhcpdiscover 广播后，它会从那些还没有租出去地址范围内选择最前面的空置 IP，连同其他 TCP/IP 设定，回应给客户端一个 Dhcpoffer 包。根据服务器端的设定，Dhcpoffer 封包会包含一个租约期限的信息。

③ 接受 IP 租约。客户端可能会收到网络上多台 DHCP 服务器的回应，此时挑选最先抵达的那个 Dhcpoffer，并且会向网络发送一个 Dhcprequest 广播封包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。

④ 租约确认。当 DHCP 服务器接收到客户端的 Dhcprequest 之后，会向客户端发出一个 Dhcpack 回应，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。

【问题 2】

由题目可知，局域网的 IP 地址为 61.100.13.0/24，可供分配的地址范围为 61.100.13.1～61.100.13.254。由于 61.100.13.252、61.100.13.253、61.100.13.254 分别分配给了路由器接口和服务器，故实际可供分配的地址范围为 61.100.13.1～61.100.13.251。因此，【起始 IP 地址】处应填入 61.100.13.1，【结束 IP 地址】处应填入 61.100.13.251，此时不需要添加排除地址。如果空(8)填入 61.100.13.254，也是正确的，这是因为 DHCP 服务器配置地址池的过程中可以定义服务器不分配的 IP 地址，可将 61.100.13.252～61.100.13.254 添加在排除的地

址范围，如图 2-138 所示。

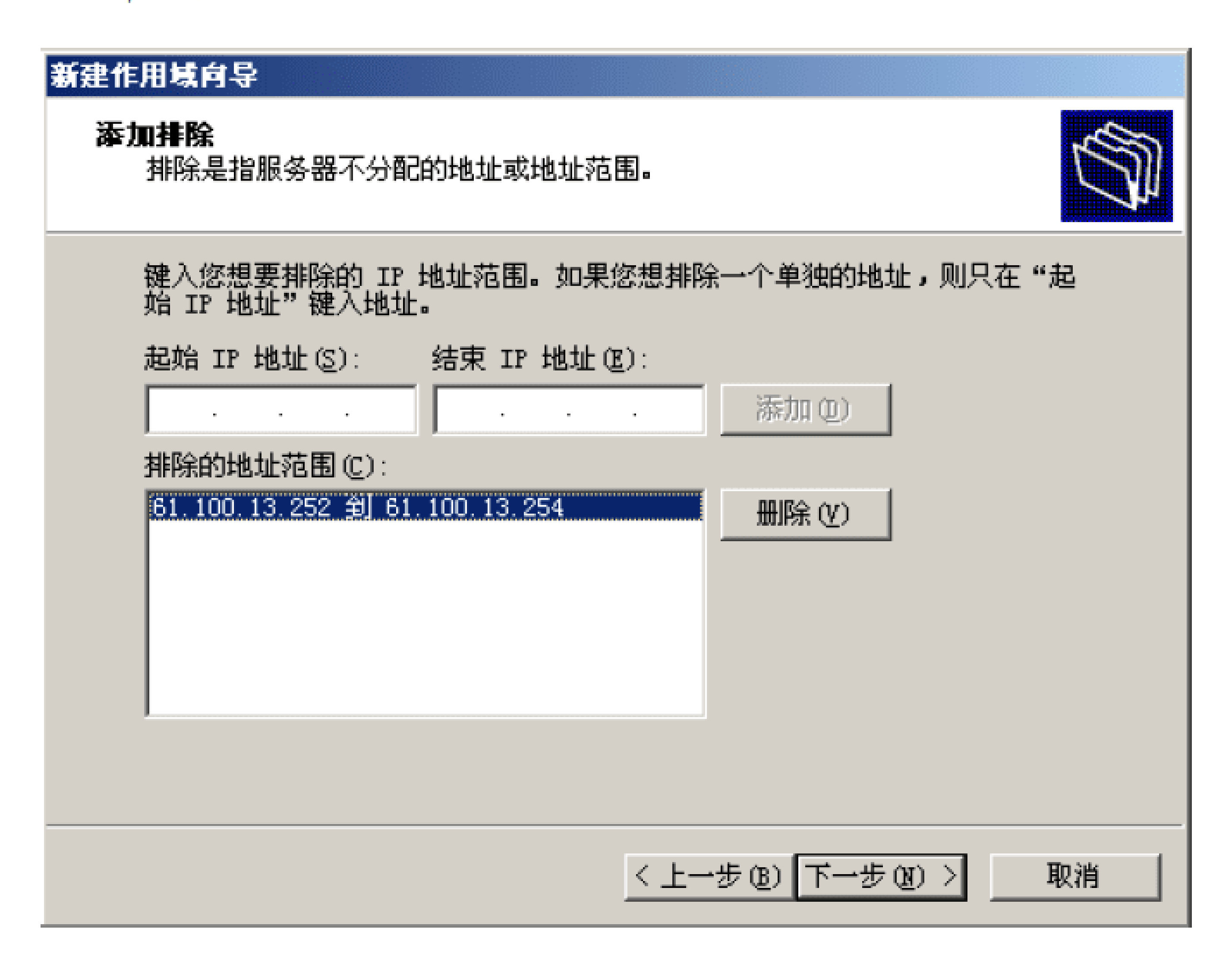


图 2-138 【新建作用域向导】对话框

【问题 3】

采用 DHCP 协议的客户端需要自动获取 IP 地址，无须客户手动配置，只需分别选中【自动获得 IP 地址】和【自动获得 DNS 服务器地址】单选按钮即可。

【问题 4】

空(9)处要填入的是网关地址。从图 2-133 中可以看出，该局域网的网关地址为 61.100.13.252，故空(9)处应填入 61.100.13.252。同时，从图 2-137 中可以看出，61.100.13.21 为 IPv4 地址，f:e80::21f:d0ff:fe83:aa0f 为 IPv6 地址，这表明 PC1 既配置了 IPv4 协议，又配置了 IPv6 协议，故空(10)应选 C。

答案：

【问题 1】

(1) A (2) B (3) C (4) D (5) 0.0.0.0 (6) 255.255.255.255

【问题 2】

(7) 61.100.13.1 (8) 61.100.13.251(或 61.100.13.254)

【问题 3】

选中【自动获得 IP 地址】单选按钮并选中【自动获得 DNS 服务器地址】单选按钮。

【问题 4】

(9) 61.100.13.252 (10) C

例 2 阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2007 年 5 月下午试题二)

【说明】

某局域网的 IP 地址为 202.117.12.0/24，网络结构如图 2-139 所示。采用 DHCP 服务器自动分配 IP 地址，其中 DHCPServer2 的地址池为 202.117.12.3～202.117.12.128。

图 2-140 和图 2-141 分别是 DHCPServer1 中 DHCP 服务器安装时分配 IP 地址的范围窗

口和添加排除界面。

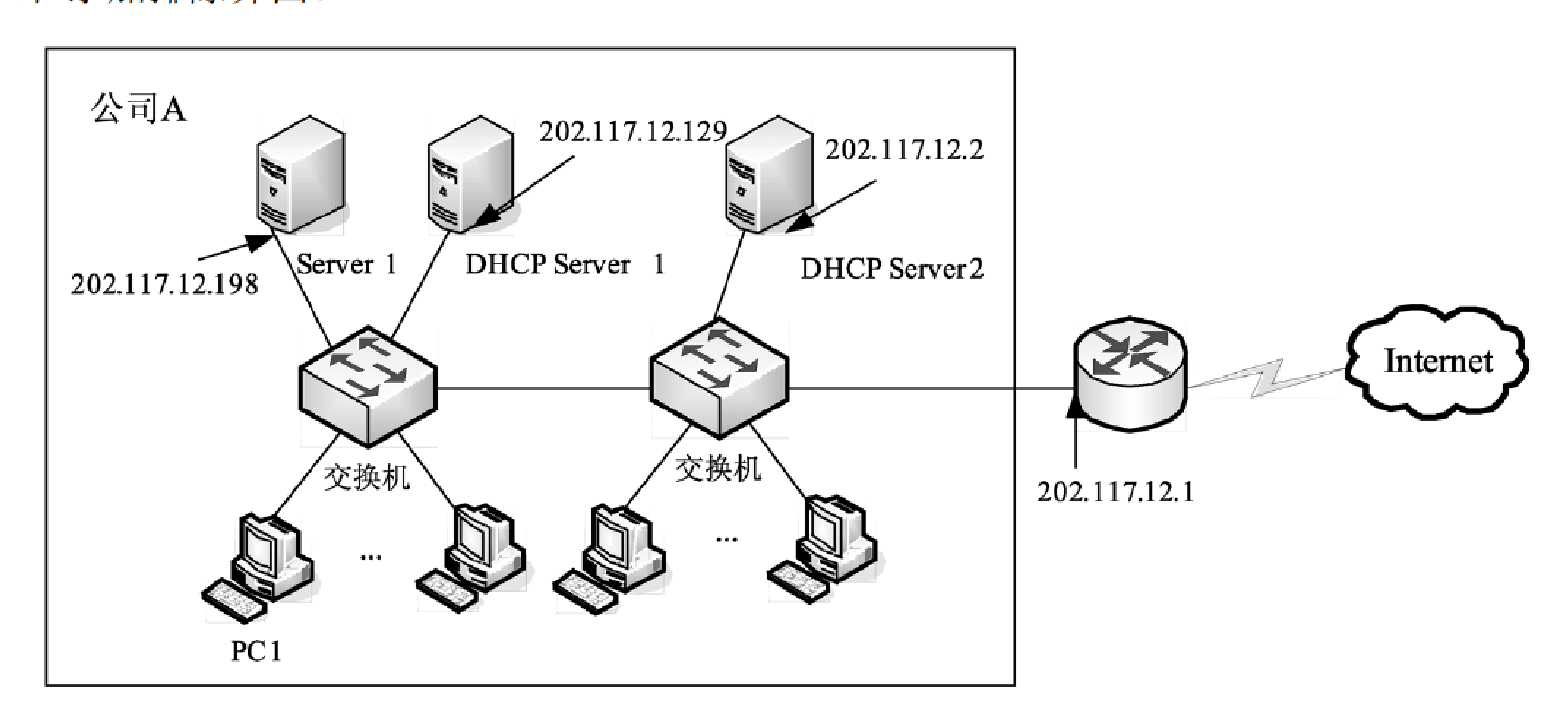


图 2-139　某局域网网络结构图

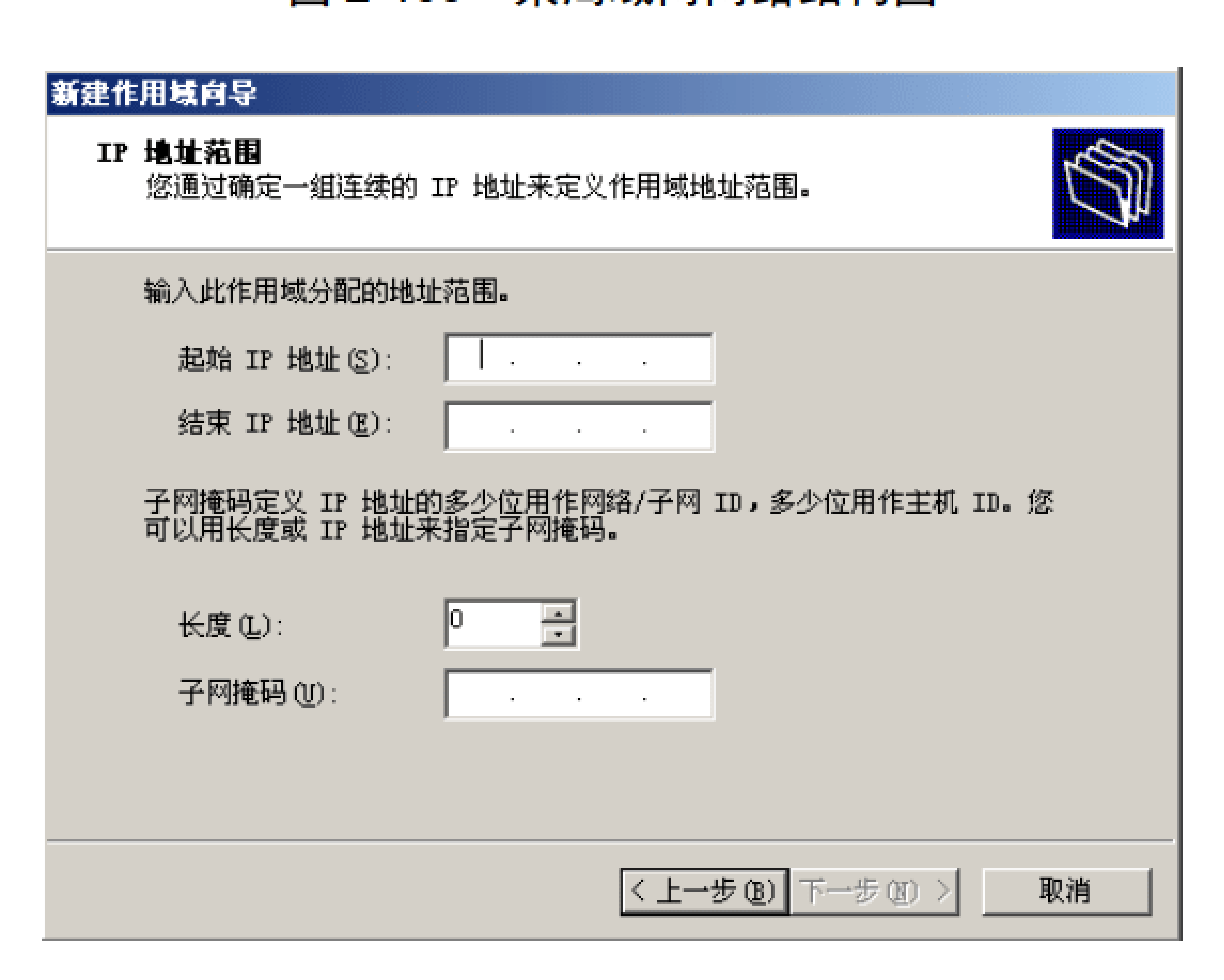


图 2-140　【IP 地址范围】界面

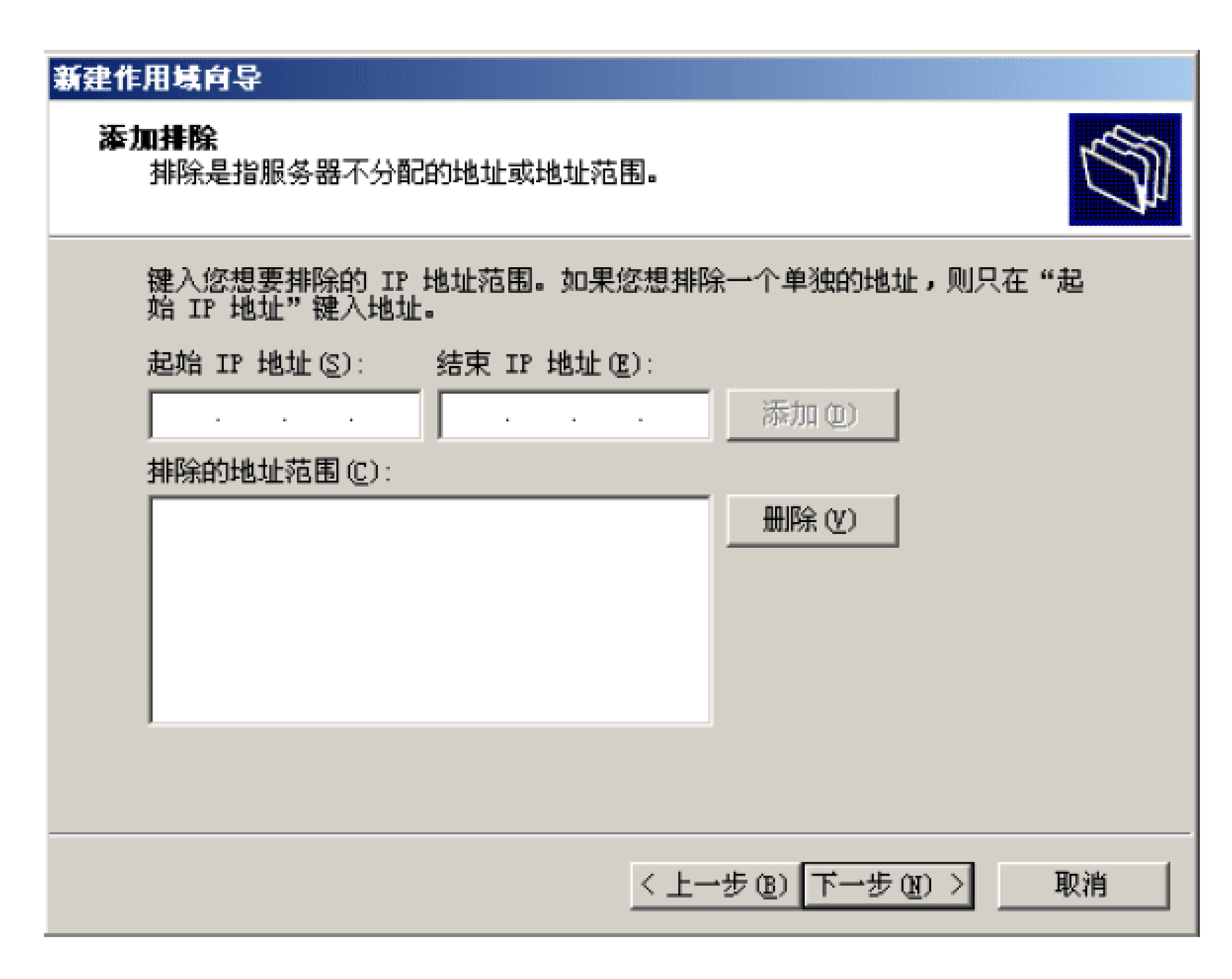


图 2-141　【添加排除】界面

图 2-142 是 DHCPServer1 中 DHCP 服务器安装时路由器(默认网关)界面。

新建作用域向导
路由器(默认网关)
您可为指定此作用域要分配的路由器或默认网关。
要添加客户端使用的路由器的 IP 地址，请在下面输入地址。
IP 地址(P):
添加(D)
删除(R)
上移(U)
下移(O)
< 上一步(B) 下一步(N) > 取消

图 2-142 【路由器(默认网关)】对话框

【问题 1】(4 分)

PC1 首次启动时，会向网络发出一个__(1)__数据包来表达 IP 租用请示，PC1 通常采用__(2)__提供的 IP 地址。

(1) A. Dhcpdiscover　　B. Dhcpoffer
　　C. Dhcprequest　　D. Dhcpdeclinf

(2) A. DHCPServer1　　B. DHCPServer2
　　C. 响应包最先到达的 DHCP 服务器

【问题 2】(3 分)

参照 DHCPServer2 的地址池分配方式，在图 2-140 中为 DHCPServer1 配置属性参数。

起始 IP 地址：　__(3)__

结束 IP 地址：　__(4)__

如果【长度】属性参数设置为 24，则系统会自动设置的子网掩码为__(5)__。

【问题 3】(2 分)

图 2-141 中的【起始 IP 地址】文本框中应填入__(6)__。

【问题 4】(2 分)

图 2-142 中 IP 地址参数应设置为：__(7)__。

【问题 5】(4 分)

PC1 可以通过运行__(8)__命令手工释放 IP 地址，运行__(9)__命令重新申请 IP 地址。

(8) A. ipconfig/giveup　　B. ipconfig/release
　　C. ipconfig/recall　　D. ipconfig/renew

(9) A. ipconfig/giveup　　B. ipconfig/release
　　C. ipconfig/recall　　D. ipconfig/renew

分析：

【问题 1】

DHCP 服务的工作过程如下。

① 当 DHCP 客户机首次启动时，客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包，该数据包表达了客户机的 IP 租用请示。

② 当 DHCP 服务器接收到 Dhcpdiscover 数据包后，该服务器从地址范围中向那台主机提供(dhcpoffer)一个还没有被分配的有效的 IP 地址。当用户的网络中包含不止一个 DHCP 服务器时，主机可能收到好几个 dhcpoffer，在大多数情况下，主机或客户机接收到的是第一个 dhcpoffer。

③ 该 DHCP 服务器向客户机发送一个确认(dhcppack)，该确认中已经包括了最初发送的 IP 地址和该地址的一个稳定期间内的租约(默认情况是 8 天)。

④ 当租约期过了一半时，客户机将和设置它的 TCP/IP 配置的 DHCP 服务器更新租约。当租期过了 87.5%时，如果客户机仍然无法与当初的 DHCP 服务器联系上，它将与其他 DHCP 服务器通信。如果网络上再没有任何 DHCP 服务器在运行，该客户机必须停止使用该 IP 地址，并从发送一个 Dhcpdiscover 数据包开始，再一次重复整个过程。

通常情况下，客户机采用响应包最先到达的 DHCP 服务器提供的 IP 地址。

【问题 2】

局域网内可用的 IP 地址为 202.117.12.1～202.117.12.254，地址 202.117.12.1 为默认网关，202.117.12.2 被分配给 DHCPServer2，202.117.12.129 被分配给 DHCPServer1，202.117.12.198 被分配给 Server1。那么可以分配给 PC 的 IP 地址范围为 202.117.12.3～202.117.12.128，202.117.12.130～202.117.12.197，202.117.12.199～202.117.12.254。已知 DHCPServer2 的地址池为 202.117.12.3～202.117.12.128，可知 DHCPServer1 的地址池为 202.117.12.130～202.117.12.254，排除地址为 202.117.12.198。

因此 DHCPServer1 配置属性参数如下。

起始 IP 地址：　202.117.12.130

结束 IP 地址：　202.117.12.254

如果【长度】属性参数设置为 24，则系统会自动设置的子网掩码为 255.255.255.0。

【问题 3】

由问题 2 的分析可知，要排除的 IP 地址为 202.117.12.198，因此图 2-141 中的【起始 IP 地址】文本框中填入 202.117.12.198。

【问题 4】

路由器的 IP 地址为 202.117.12.1，故图 2-142 中 IP 地址参数应设置为 202.117.12.1。

【问题 5】

ipconfig 诊断命令显示所有当前的 TCP/IP 网络配置值。

ipconfig 命令格式如下：

```
ipconfig [/all /renew [adapter] /release [adapter]]
```

其中各参数说明如下。

参数/all：产生完整显示。在没有该开关的情况下 ipconfig 只显示 IP 地址、子网掩码和每个网卡的默认网关值。

参数/renew [adapter]：更新 DHCP 配置参数。该选项只在运行 DHCP 客户端的系统上可用。要指定适配器名称，则输入使用不带参数的 ipconfig 命令显示的适配器名称。

参数/release [adapter]：发布当前的 DHCP 配置。该选项禁用本地系统上的 TCP/IP，并只在 DHCP 客户端上可用。要指定适配器名称，则输入使用不带参数的 ipconfig 命令显示的适配器名称。

答案：

【问题 1】

(1) A　　(2) C

【问题 2】

(3) 202.117.12.130　　(4) 202.117.12.254　　(5) 255.255.255.0

【问题 3】

(6) 202.117.12.198

【问题 4】

(7) 202.117.12.1

【问题 5】

(8) B　　(9) D

2.7.3 同步练习

1．阅读以下说明，回答问题 1～问题 5，将答案填入对应的解答栏内。

【说明】

某公司在国际网络互联中心申请了一个 C 类 IP 地址 210.45.12.0/24，域名为 abc.com.cn。该公司没有划分子网，使用一台 Cisco 2610 路由器接入互联网，其接入内部局域网的 IP 地址是 210.45.12.99，并有一台 DNS 服务器(210.45.12.10)、一台 Web 服务器(210.45.12.100)、一台 FTP 服务器(210.45.12.101)和一台 MAIL 服务器(210.45.12.102)。

原来该公司采用手工分配 IP 地址，现要改用 DHCP 自动分配 IP 地址，拟使用一台安装有 Windows Server 2003 的 PC 服务器作为 DHCP 服务器，它的 IP 地址为 210.45.12.103。若你是该公司的网络管理员，需要配置这台 DHCP 服务器。假设该公司不会有新服务器，把所有的地址都动态地分配给客户机。

【问题 1】该作用域的 IP 地址范围是什么？子网掩码是多少？

【问题 2】排除范围是什么？

【问题 3】默认网关是什么？

【问题 4】域名是什么？域名服务器 IP 地址是什么？

【问题 5】该公司销售部有一台 PC，由于其工作性质决定了必须有一个固定 IP 地址，你如何给它分配一个固定 IP 地址？(写出两种方案)

2．阅读以下说明，回答问题 1～问题 6，将答案填入对应的答案栏内。

【说明】

某公司在国际网互联中心申请了一个 C 类的 IP 地址 210.45.12.0/24，域名为 abc.com.cn，其 DNS 服务器的地址是 210.45.12.103。该公司没有划分子网，使用一台 Cisco 2610 路由器接入互联网，其接入内部局域网的 IP 地址是 210.45.12.1。

原来该公司采用手工分配 IP 地址，现要改用 DHCP 自动分配 IP 地址，拟使用一台安装有 RedHat Linux 的 PC 服务器作为 DHCP 服务器。该公司准备把 210.45.12.20～210.45.12.120 和 210.45.12.150～210.45.12.250 这两块地址用于动态分配给客户机，其他地址用作服务器 IP 或保留下来以便网络扩充。下面是 DHCP 服务配置文件/etc/dhcpd.conf 的主要内容：

```
subnet 210.45.12.0 netmask 255.255.255.0 {
____________(1)____________;
range 210.45.12.150     210.45.12.250;
default-lease-time 86400;
max-lease-time 604800;
option subnet-mask 255.255.255.0;
option routers ________(2)________;
option domain-name "________(3)________";
option broadcast-address 200.117.207.255;
option domain-name-servers ________(4)________
host mypc {
hardware ethernet 00:0a:e6:b2:2f:5b;
fixed-address 210.45.12.215;
}
}
```

【问题 1】(1)处应当填写什么内容？

【问题 2】(2)处应当填写什么内容？

【问题 3】(3)处应当填写什么内容？

【问题 4】(4)处应当填写什么内容？

【问题 5】文件/etc/dhcpd.conf 中阴影部分的含义是什么？

【问题 6】文件/var/state/dhcp/dhcpd.leases 在 DHCP 中起什么作用？

3．阅读以下说明，回答问题 1～问题 5，将答案填入对应的答案栏内。

【说明】

在 Linux 下安装配置 DHCP 服务，DHCP 服务程序/usr/sbin/dhcpd 需要读取配置文件/etc/dhcpd.conf，以下是一个 DHCP 配置文件的主要内容：

```
subnet 210.45.12.0 netmask 255.255.255.0 {
range 210.45.12.40  210.45.12.120;
range 210.45.12.150 210.45.12.225;
default-lease-time 86400;
max-lease-time 604800;
option subnet-mask 255.255.255.0;
option routers 210.45.12.254;
option domain-name "xyz.com.cn";
option broadcast-address 210.45.12.255;
option domain-name-servers 210.45.12.10;
}
```

【问题 1】此配置允许 DHCP 服务器给客户的地址范围是什么？

【问题 2】如果客户机连续请求继续租约 IP 地址都失败，那么它在租用 IP 地址最长时间是多少秒？

【问题 3】DHCP 服务器发送给客户机的信息中子网掩码是什么？DNS 服务器的地址是什么？路由器的地址是什么？

【问题 4】配置完毕后，可以用什么命令启动 DHCP 服务？(不重新启动计算机)

【问题 5】在 Linux 下配置 DHCP 服务，必须创建一个名为 dhcpd.leases 的 DHCP 客户租约数据库文件，其命令是什么？

2.7.4 同步练习参考答案

1．

【问题 1】该作用域的 IP 地址范围是 210.45.12.1～210.45.12.254；子网掩码为 255.255.255.0。

【问题 2】210.45.12.10、210.45.12.99～210.45.12.103。

【问题 3】210.45.12.99。

【问题 4】域名为 abc.com.cn 域名服务器 IP 地址是 210.45.12.10。

【问题 5】第一种方法是把要分配给该主机的 IP 地址加入排除范围之内；第二种方法是保留特定的地址，这时要输入保留名称、保留 IP 地址和该主机网卡的 MAC 地址。

2．

【问题 1】range 210.45.12.20　210.45.12.120。

【问题 2】210.45.12.1。

【问题 3】abc.com.cn。

【问题 4】210.45.12.103。

【问题 5】把 210.45.12.215 固定地分配给 mypc 这台主机，这台主机网卡的 MAC 地址是 00:0a:e6:b2:2f:5b。

【问题 6】它是 DHCP 客户租约的数据库文件，用于存放 IP 地址租约信息。

3．

【问题 1】210.45.12.40～210.45.12.120 和 210.45.12.150～210.45.12.225。

【问题 2】604800。

【问题 3】子网掩码是 255.255.255.0；DNS 服务器的地址是 210.45.12.10；路由器的地址是 210.45.12.254。

【问题 4】/etc/rc.d/init.d/dhcpd restart。

【问题 5】# touch /var/state/dhcp/dhcpd.leases。

2.8 本 章 小 结

本章知识点在 2009 年的新大纲中变化较小，主要删除了 Linux 环境下各种服务器的配

置和维护。

本章知识点非常多，也是下午考试的重点之一。由于对应用服务器的配置是一个实践性很强的工作，考生在复习本章时，应该尽可能亲手配置一下这些服务，这样印象会更深，学习起来能够理论联系实际，能更有效地掌握本章的知识。同时要注意配合《网络管理员考试同步辅导(计算机与网络基础知识篇)》第 5 章介绍的各种服务器基础知识一起学习。

本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目基本上涵盖了大纲规定的知识要点。

2.9　达标训练题及参考答案

2.9.1　达标训练题

1．阅读以下说明，回答问题 1～问题 3，将答案填入对应的答案栏内。

【说明】

某单位有一个网络，其中有一台主机的 IP 地址是 190.190.147.134。请回答以下问题。

【问题 1】这个地址是一个什么类型的地址？不划分子网时，其网络地址是多少？广播地址是什么？

【问题 2】它的默认子网掩码是什么？

【问题 3】若子网掩码是 255.255.240.0，则这台主机所在的子网地址是什么？该子网的广播地址是什么？这个 IP 地址所在的子网的主机 IP 范围是什么？

2．阅读以下说明，回答问题 1～问题 4，将解答填入对应的答案栏内。

【说明】

某公司申请了一个 C 类地址 196.102.56.0，公司有生产部门、市场部门、财务部门、人事部门、技术部门和经理办公室，每个部门都需要划分为单独的网络，即需要划分至少 5 个子网，每个子网至少支持 24 台主机。(使用固定子网掩码)

【问题 1】应将子网掩码设置为什么？

【问题 2】每个子网有多少个主机地址？

【问题 3】196.102.56.197 所在子网的网络地址是什么？

【问题 4】196.102.56.197 所在子网的广播地址是什么？

3．阅读以下说明，回答问题 1～问题 3，将解答填入对应的答案栏内。

【说明】

某一小型公司从 ISP 申请了一个 Internet 出口，ISP 给该公司提供了 5 个 IP 地址，分别是 222.34.109.66～222.34.109.70，ISP 给该公司提供的路由器地址是 222.34.109.65。

【问题 1】由于 ISP 忘记告诉子网掩码，你认为最有可能的子网掩码是什么？

【问题 2】这个子网的子网地址是什么？

【问题 3】这个子网有广播地址是什么？

4．阅读以下说明，回答问题 1～问题 3，将答案填入对应的答案栏内。

【说明】

某公司被分配了一个 C 类地址 200.100.50.0，根据需要，该公司将网络划分成若干个子网，其中：有 4 个子网，每个子网最多有主机 30 台；有 3 个子网，每个子网最多有主机 5 台；另外还有 9 个点到点串行链路。

【问题 1】请为该网络进行子网分割，至少有 3 个不同变长的子网掩码，并画出子网划分示意图。注意：该单位的路由器不支持全 0 和全 1 子网。

【问题 2】请列出你所分配的网络地址。

【问题 3】为该网络分配点到点串行链路地址。

5．阅读以下说明，回答问题 1～问题 5，将解答填入对应的答案栏内。

【说明】

某公司使用了一台安装有 Linux 操作系统的 PC 服务器作为电子邮件服务器，邮件发送服务使用的是 sendmail 8.0。下面是 sendmail 的几个配置文件的片段：

/etc/sendmail.cf 文件片段：

```
Cwlocalhost
Fw/etc/mail/local-host-names
```

/etc/mail/access 文件内容：

```
localhost.localdomain        RELAY
localhost                    RELAY
127.0.0.1                    RELAY
210.45.45                    RELAY
aapla.edu.cn                 RELAY
           (1)
```

/etc/aliases 文件内容：

```
bin:           root
daemon:        root
adm:           root
lp:            root
sync:          root
shutdown:      root
halt:          root
mail:          root
webmaster:     zhang
net_center:        zhang, taoan, liwenglong
owner-net_group: zhang
```

【问题 1】在/etc/sendmail.cf 文件中并没指定该电子邮件服务器的主机名，但它却能接收所有 abc.com.cn 域内的电子邮件，这个信息可能存放在哪儿？

【问题 2】该公司的员工最有可能在哪个网络中收发电子邮件？

【问题 3】在使用过程中，发现域 xyz.com.tw 上有人使用该服务器发送电子邮件，为了拒绝其访问，在(1)处该填写什么内容？

【问题 4】该公司主页上有一个电子邮件链接，邮件地址是 webmaster@abc.com.cn，单击它通过 Outlook Express 发送了一封电子邮件，该邮件将发送给谁？

【问题 5】命令#/usr/bin/makemap /etc/mail/access.db</etc/mail/access 的作用是什么？

6．阅读以下说明，回答问题 1～问题 5，将解答填入对应的答案栏内。

【说明】

图 2-143 是某小型公司网络拓扑结构，其中代理服务器的两块网卡的设置已在图中标出。

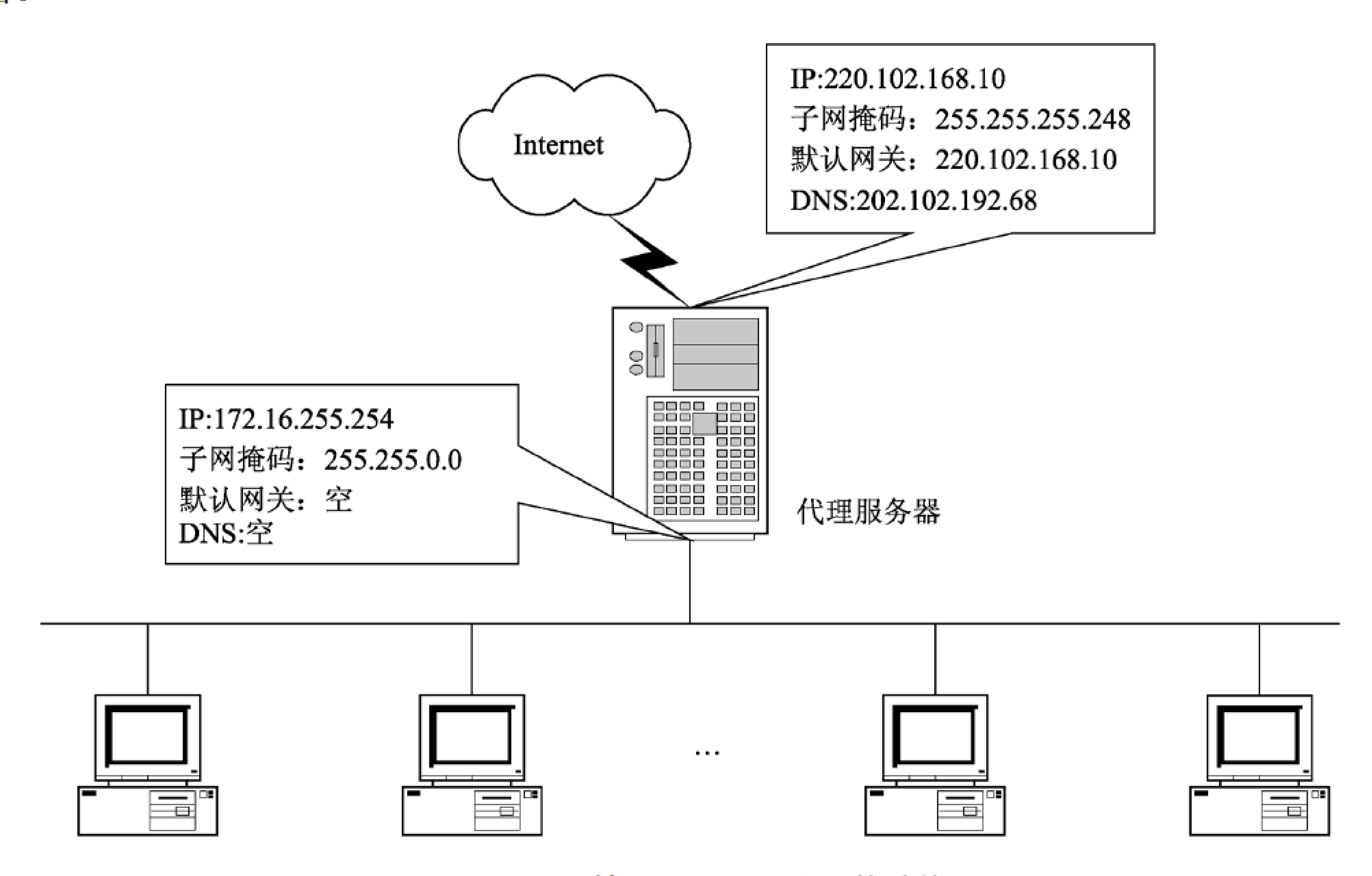


图 2-143　某小型公司网络拓扑结构

该代理服务器使用基于 Linux 的 Squid 代理服务器，下面为该服务器中文件/etc/squid/squid.conf 的一个片段。

```
http_port 8080
cache_mem 256 MB
cache_dir  /cache1 4000 24 33
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers _______(1)_______
acl denydomain dstdomain foo.com.tw
acl all scr 0.0.0.0/0.0.0.0
http_access deny denydomain
http_access allow all
cache_mgr administrator@abc.com.cn
```

【问题 1】该公司主机的 IP 地址范围是什么？子网掩码是什么？

【问题 2】客户机的 IE 的代理服务器端口号应设置为多少？(采用传统代理)

【问题 3】该代理服务器缓冲区放在哪里？大小是多少？能建多少一级目录，多少二级目录？

【问题 4】(1)处应填入什么内容？

【问题 5】文件中两行阴影语句的作用是什么？

7．某单位的网络要配置一台 DHCP 服务器，为网络内部的计算机自动分配 IP 地址。在考虑 DHCP 服务器时，回答以下问题。

【问题 1】客户机启动时是如何从 DHCP 服务器得到动态 IP 的？

【问题 2】DHCP 客户机在启动时并没有 IP 地址，也不知道 DHCP 服务器的地址，那么它与 DHCP 服务器之间是通过什么方式进行通信的？

【问题 3】配置 DHCP 服务器应具备什么条件？

【问题 4】Windows 2000 用户通过什么命令可以看到自己租约到的本机 IP 地址？用何命令可以重新向 DHCP 服务器租约 IP？用何命令可以释放 IP？

8．阅读以下说明，回答问题 1～问题 5，将解答填入对应的答案栏内。

【说明】

在 Linux 下安装、配置 Apache 服务，Apache 服务程序 httpd 启动时需要读取配置文件 httpd.conf。以下是 httpd.conf 配置文件的一个片段：

```
## httpd.conf -- Apache HTTP server configuration file
### Section 1: Global Environment
ServerType standalone
ServerRoot "/etc/httpd"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MaxClients 150
### Section 2: 'Main' server configuration
Port 80
User apache
Group apache
ServerAdmin webmaster@abc.com.cn
ServerName www.abc.com.cn
DocumentRoot "/var/www/html"
UserDir public_html
DirectoryIndex index.html
Alias /jianji "/home/zhang/jianji"
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument 404 /missing.html
### Section 3: Virtual Hosts
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
   ServerAdmin webmaster@abc.com.cn
   DocumentRoot /www/htdocs/abc
   ServerName markert.abc.com.cn
   ErrorLog logs/host.some_domain.com-error_log
   CustomLog logs/host.some_domain.com-access_log common
</VirtualHost>
```

【问题 1】该 Web 服务器的工作目录是什么？

【问题 2】当用户要访问该 Web 服务器的一个文件时，这个文件已经被删除了，服务器该如何响应客户？

【问题 3】httpd.conf 文件中阴影部分语句的作用是什么？

【问题 4】当用户在浏览器中输入 http:// 192.168.10.100/zhang/时，将访问什么内容？

【问题 5】停止 Apache 服务器的命令是什么？

2.9.2　参考答案

1.

【问题 1】B 类地址、190.190.0.0、190.190.255.255

【问题 2】255.255.0.0

【问题 3】190.190.144.0、190.190.159.255、190.190.144.1～190.190.159.254

2.

【问题 1】255.255.255.224

【问题 2】30

【问题 3】196.102.56.192

【问题 4】196.102.56.223

3.

【问题 1】255.255.255.248

【问题 2】222.34.109.64

【问题 3】222.34.109.71

4.

【问题 1】255.255.255.224、255.255.255.248 和 255.255.255.252；图 2-144 是一种划分方法：

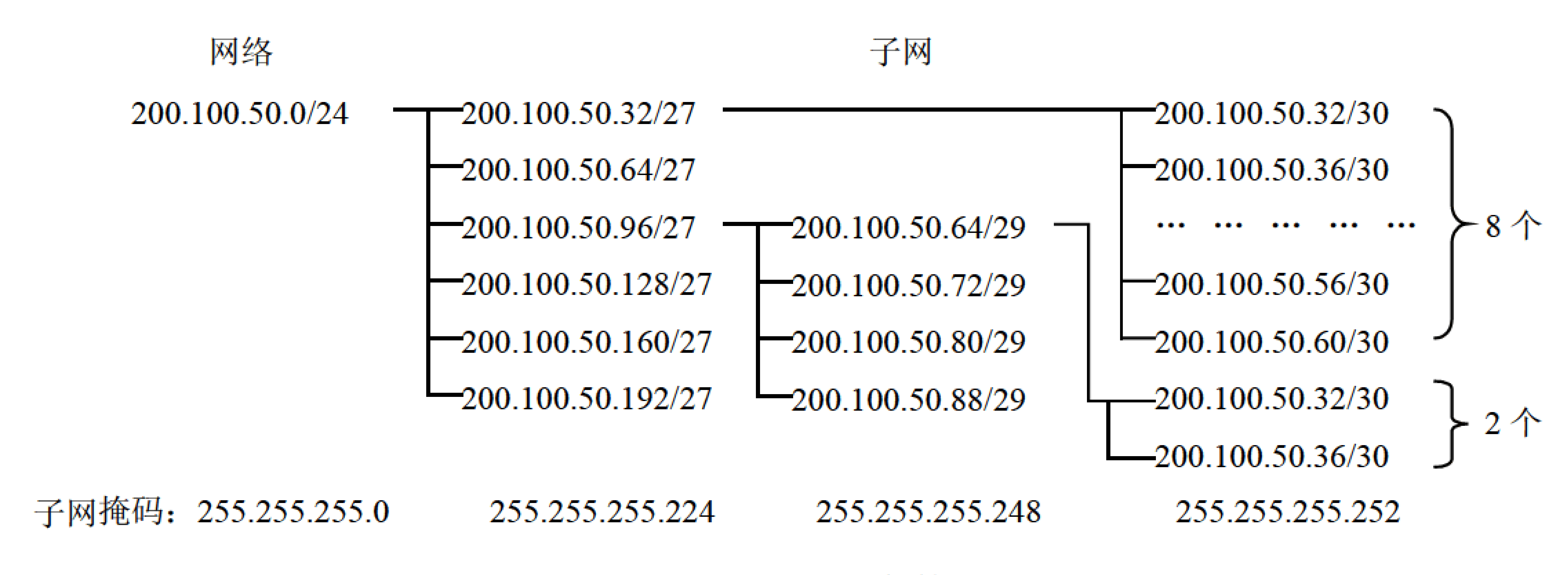


图 2-144　问题 1 解答

【问题 2】见问题 1

【问题 3】见问题 1

5.

【问题 1】存放在/etc/mail/local-host-names 文件中

【问题 2】210.45.45.0/24 这个 C 类网络中

【问题 3】xyz.com.tw　DENY

【问题 4】将发给 zhang 这个用户，邮件服务器地址是 zhang@abc.com.cn

【问题 5】创建传送控制配置文件 Access 相应的数据库文件

6.

【问题 1】172.16.0.1～172.168.255.253、255.255.0.0

【问题 2】8080

【问题 3】/cache1、4000MB、24、33

【问题 4】202.102.192.68

【问题 5】禁止客户访问域 foo.com.tw 内的所有主机

7.

【问题 1】请求 IP 租约、提供 IP 租约、选择 IP 租约和确认 IP 租约

【问题 2】广播方式

【问题 3】DHCP 服务器应具有静态 IP 和子网掩码，有一组可供分配的 IP 地址。

【问题 4】ipconfig/all、ipconfig/renew、ipconfig/release

8.

【问题 1】/etc/httpd

【问题 2】用文档/missing.html 来回应客户浏览器

【问题 3】建立一个域名为 markert.abc.com.cn 的虚拟 Web 服务器(虚拟主机)，并指定相应的参数。

【问题 4】访问该服务器中用户 zhang 的主目录下 public_html 子目录的索引文件 index.html，若该文件不存在就会出错。

【问题 5】#/etc/init.d/httpd stop

第 3 章　网络安全设置

大纲要求：

- 防火墙技术和入侵检测系统，包括防火墙的配置策略、入侵处理策略、漏洞处理策略。
- 病毒及病毒防范。
- 加密、认证、数字签名等安全技术，包括 DES 和 RSA 的基本概念、认证、数字证书、安全电子邮件、HTTPS。

3.1　网络病毒防护策略和入侵处理策略

3.1.1　考点辅导

3.1.1.1　网络病毒简介

1. 什么是网络病毒

网络病毒是指在网络上传播的计算机病毒，可能会为网络带来灾难性的后果，被称为“第二代病毒”。

2. 网络病毒的特点

网络病毒的特点及危害性主要表现在：破坏性强、传播性强、具有潜伏性和可激发性、针对性强、扩散面广、传播速度快、难以彻底清除等。

3. 黑客的攻击手段

涉及网络安全的问题很多，但最主要的问题还是人为攻击，黑客就是最具有代表性的一类群体。黑客的出现可以说是当今信息社会，尤其是在因特网互联全球的过程中，网络用户有目共睹、不容忽视的一个独特现象。

常见的黑客攻击手段有以下几个。

1)　口令入侵

口令入侵是指使用某些合法用户的帐号和口令登录到目的主机，然后再实施攻击活动。使用这种方法的前提是必须先得到该主机上的某个合法用户的帐号，然后再进行合法用户口令的破译。通常，黑客会利用一些系统使用习惯性的帐号的特点，采用字典穷举法(或称暴力法)来破解用户的密码。

2)　放置特洛伊木马程序

从严格的定义来讲，凡是非法驻留在目标计算机中，在目标计算机系统启动的时候自动运行，并在目标计算机上执行一些事先约定的操作(如窃取口令等)的程序都可以称为特洛

伊木马程序，即 Trojans。

特洛伊木马程序一般分为服务器端(Server)和客户端(Client)。服务器端是攻击者传到目标机器上的部分，用来在目标机上监听，以等待客户端连接过来；客户端是用来控制目标机器的部分，放在攻击者的机器上。

3) DoS 攻击

造成 DoS (Denial of Service，拒绝服务)的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击是指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终导致计算机无法再处理合法的用户请求。

分布式拒绝服务(Distributed Denial of Service，DDoS)攻击是指借助于客户机/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。

4) 端口扫描

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。常用的扫描方式有 TCP connectU 扫描、TCP SYN 扫描、TCP FIN 扫描、IP 段扫描和 FTP 返回攻击等。

5) 网络监听

网络监听在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因而一直备受网络管理员的青睐。然而，另一方面网络监听也给以太网的安全带来了极大的隐患，许多的网络入侵往往都伴随着以太网内的网络监听行为，从而造成口令失窃，敏感数据被截获等连锁性安全事件。

Sniffer 是一个著名的监听工具，它可以监听到网上传输的所有信息。Sniffer 可以是硬件也可以是软件，主要用来接收在网络上传输的信息。

6) 欺骗攻击

欺骗攻击是攻击者创造一个易于误解的上下文环境，以诱使受攻击者进入并且做出缺乏安全考虑的决策。

常见的欺骗攻击如下。

(1) Web 欺骗。Web 欺骗允许攻击者创造整个 WWW 世界的影像副本。影像 Web 的入口进入到攻击者的 Web 服务器，经过攻击者机器的过滤作用，允许攻击者监控受攻击者的任何活动，包括帐户和口令。攻击者观察和控制着受攻击者在 Web 上所做的每一件事。

(2) ARP 欺骗。通常源主机在发送一个 IP 包之前，它要到该转换表中寻找和 IP 包对应的 MAC 地址。此时，若入侵者强制目的主机 Down 掉(如发洪水包)，同时把自己主机的 IP 地址改为合法目的主机的 IP 地址，然后它发一个 ping (icmp 0)给源主机，要求更新主机的 ARP 转换表，主机找到该 IP，然后在 ARP 表中加入新的 IP->MAC 对应关系。这样合法的目的主机就失效了，入侵主机的 MAC 地址变成了合法的 MAC 地址。

(3) IP 欺骗。IP 欺骗由若干步骤组成。首先，目标主机已经选定；其次，信任模式已被发现，并找到了一个被目标主机信任的主机。黑客为了进行 IP 欺骗，需要进行以下工作：

使得被信任的主机丧失工作能力，同时采样目标主机发出的 TCP 序列号，从而猜测出它的数据序列号。然后，伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

7)　电子邮件攻击

电子邮件攻击主要表现为向目标信箱发送电子邮件炸弹。所谓邮件炸弹实质上就是发送地址不详且容量庞大的垃圾邮件。因为相对于其他的攻击手段来说，这种攻击方法具有简单、见效快等优点。

电子邮件欺骗也是黑客常用的手段。他们常会佯称自己是系统管理员(邮件地址和系统管理员完全相同)，给用户发送邮件，要求用户修改口令(口令有可能为指定的字符串)或在貌似正常的附件中加载病毒或某些特洛伊木马程序。

3.1.1.2　基于网络的防病毒系统

1.　网络防病毒需求

目前，Internet 已经成为病毒传播的最大途径，电子邮件和网络信息的传递为病毒传播打开了高速的通道。各行各业网络化的发展也使病毒的传播速度大大提高，感染的范围也越来越广。可以说，网络化带来了病毒的高效率，而病毒的高效率也对防病毒产品提出了新的要求。

2.　网络病毒传播方式

一般来说，计算机网络的基本构成为网络服务器和网络节点站(包括有盘工作站、无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘，然后进入网络，进一步在网上传播。具体来说，其传播方式有如下几种。

(1)　病毒直接从有盘工作站复制到服务器中。

(2)　病毒先传染工作站，在工作站内存中驻留，等运行网络盘内程序时再传染给服务器。

(3)　病毒先传染工作站，在工作站内存中驻留，在运行时直接通过映像路径传染到服务器。

(4)　如果远程工作站被病毒侵入，病毒也可以通过通信过程中的数据交换进入网络服务器中。

3.　网络病毒防护策略

基于网络系统的病毒防护体系主要包括以下几个方面的策略。

1)　一定要实现全方位、多层次防毒

一定要部署多层次病毒防线，如网关防毒，群件服务器、应用服务器防毒和客户端防毒，保证斩断病毒可以传播、寄生的每一个节点，从而实现病毒的全面防范。

2)　网关防毒是整体防毒的首要防线

将网关防毒作为最重要的一道防线来部署，全面消除外来病毒的威胁，使得病毒不再从网络传播进来，以免对内部网资源和系统资源造成消耗。同时，网关防毒这道防线还必须具备内容过滤功能，以全面防范垃圾邮件的侵扰以及内部机密数据的外泄。

3) 缺乏管理的防毒系统是无效的防毒系统

为保证防毒系统有效、及时地拦截病毒，必须确保整个防毒产品可以从管理系统中及时得到更新，整个系统中任何一个节点都可以被管理人员随时管理。

4) 技术支持服务是整体防毒系统中极为重要的一环

病毒破坏系统的方法多种多样，病毒传播和感染的多种手段，新的病毒对防病毒软件自身破坏情况的增多，这些都造成防病毒软件在具体实施和应用中会遇到各种各样的问题。因此，防病毒厂商能否及时、全面地提供解决方案及技术支持服务是能不能对网络病毒进行有效防范极为重要的一环，另一方面要求厂商能有足够的本地化技术人员作为依托。

4. 网络防毒系统的组织形式

1) 系统中心统一管理

为了提高杀毒的效率和稳定性，可采用多级管理体系，由系统中心统一管理。中心可以控制网络内的所有机器统一杀毒，在同一时间查杀所有病毒，从而解决网络环境下机器的重复感染问题。

2) 远程安装升级

网络病毒防护系统提供远程安装和用户通过 Web 页面下载客户端自行安装两种方式，客户端能自动从系统中心升级。

3) 一般客户端的防毒

系统中心可以控制客户端的杀毒软件，由系统中心统一组织杀毒；客户端也可自行查杀，并将结果报送系统中心。服务器端的查杀操作应与客户端一致，区别在于软件是为服务器专门设计的杀毒软件。

4) 防病毒过滤网关

防病毒过滤网关实际上就是企业级病毒防火墙，通常通过部署在用户内部网与外部网的接入点，实现邮件病毒过滤及 Internet 病毒过滤。它可以简单、高效地对用户网络可能遇到的来自 Internet 的病毒威胁提供强有力的深层病毒防护。

5) 硬件防病毒网关

与客户端、服务器软件类防毒产品相比，硬件防毒网关类产品具有以下特色。

- 高效稳定。硬件防毒网关类产品由于采用独立的硬件平台，大大提高了系统的稳定性和查杀病毒的效率。
- 操作简单、管理方便。硬件防毒网关类产品一般采用 B/S 管理构架，友好的图形管理界面可供用户方便地对设备进行简单易行的配置。
- 接入方式简单易行。
- 免维护。远程自动更新代码和系统升级，无须管理员日常维护。
- 容错与集群。系统通过集群模块，在容错的同时，线性地增加处理能力，从而满足高带宽的网关杀毒需要。

3.1.1.3 入侵检测系统部署

1. 部署实例

对于入侵检测系统来说，其类型不同、应用环境不同，部署方案也就会有所差别。对于基于主机的入侵检测系统来说，一般用于保护关键主机或服务器，因此只要将它部署到

这些关键主机或服务器中即可。但是对于基于网络的入侵检测系统来说，因各种网络环境千差万别，根据网络环境的不同，其部署方案也会有所不同。

1)　共享部署

在共享介质的环境下，传感器能够监听到整个冲突域内的流量，所以只需要把传感器的监听端口接到 Hub 上即可，如图 3-1 所示。

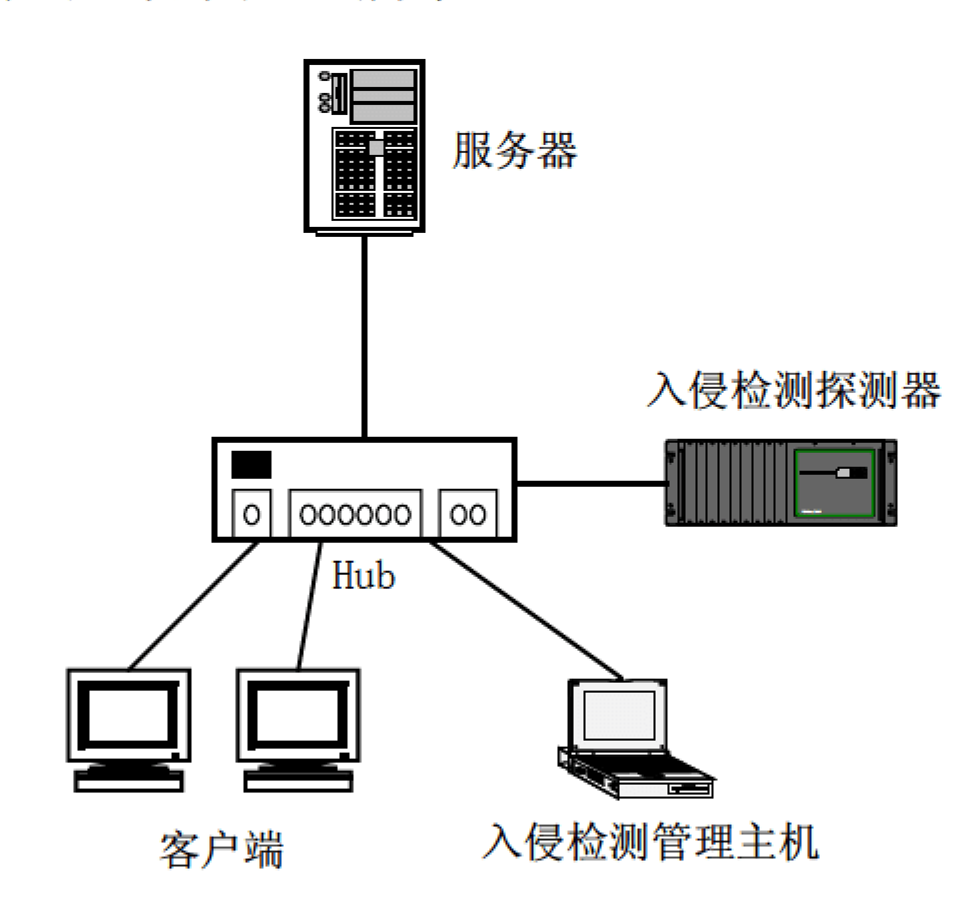


图 3-1　共享介质环境下入侵检测的部署

2)　交换环境

在交换环境下，每个交换机的端口都是一个独立的冲突域，因此传感器不能直接监听到交换机其他端口的流量。通常可以采用以下几种方法解决此问题。

- 在交换机和路由器之间接入一个 Hub，从而把一个交换环境转换为共享环境。这样做的优点是简单易行，成本低廉。如果客户对网络的传输速度和可靠性要求不高，建议采用这种方法，如图 3-2 所示。

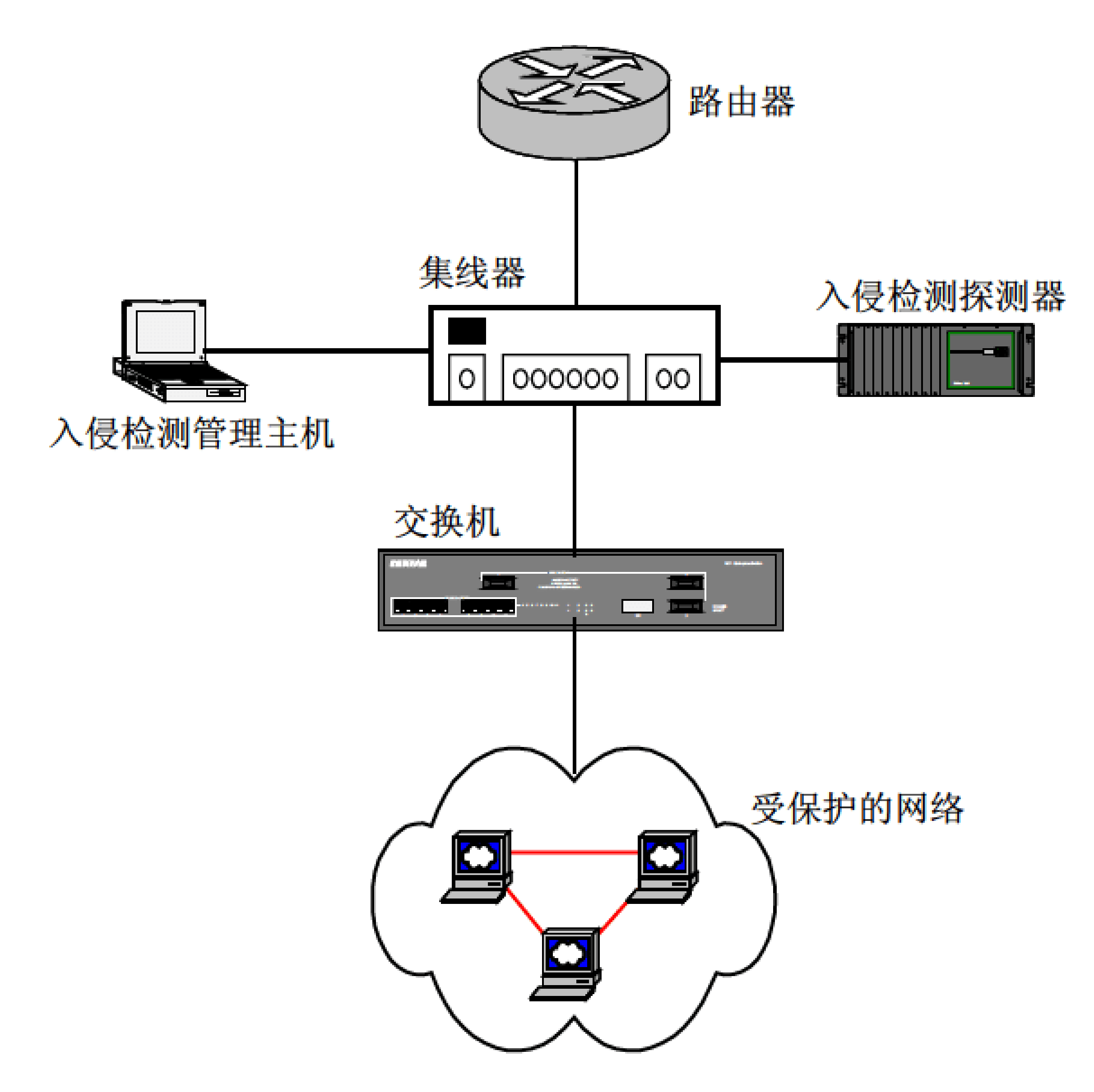


图 3-2　交换环境下接入集线器入侵检测的部署

- 如果交换机支持端口镜像功能，建议采用以下方法：在不改变原有网络拓扑结构的基础上完成传感器的部署。其优点是配置简单、灵活，使用方便，不需中断网络。这是比较常用的一种方式，如图 3-3 所示。

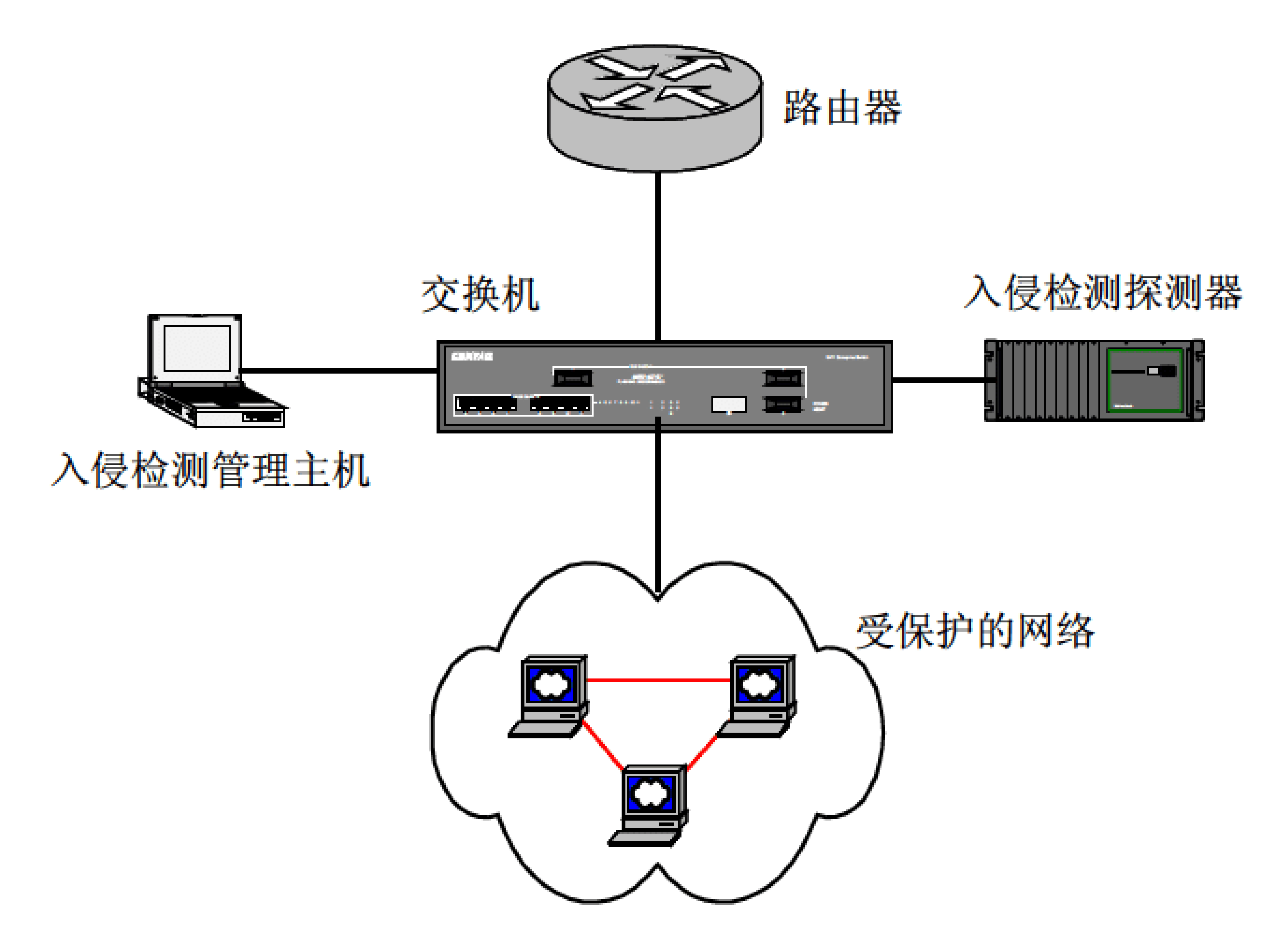


图 3-3　交换环境下入侵检测的部署

- 如果交换机不支持端口镜像功能，或者出于性能的考虑不便启用该功能，可以采用 TAP(分支器)。它的优点是能够支持全双工 100Mb/s 或者全双工 1000Mb/s 的网络流量。

2. 典型应用

本实例假设所采用的交换机支持端口镜像的功能。

1) 小规模网络环境

此种区域网连接方法较为简单，内部网络中各机构的主机使用共享式 Hub 连接到交换机上，或主机直接连接到交换机上，交换机不设 VLAN，交换机再通过路由器接入 Internet。在这种情况下，将 IDS 监测主机接到交换机的广播口(监听口)即可监听到内部网络间的所有通信及内部网络到 Internet 的所有通信，如图 3-4 所示。

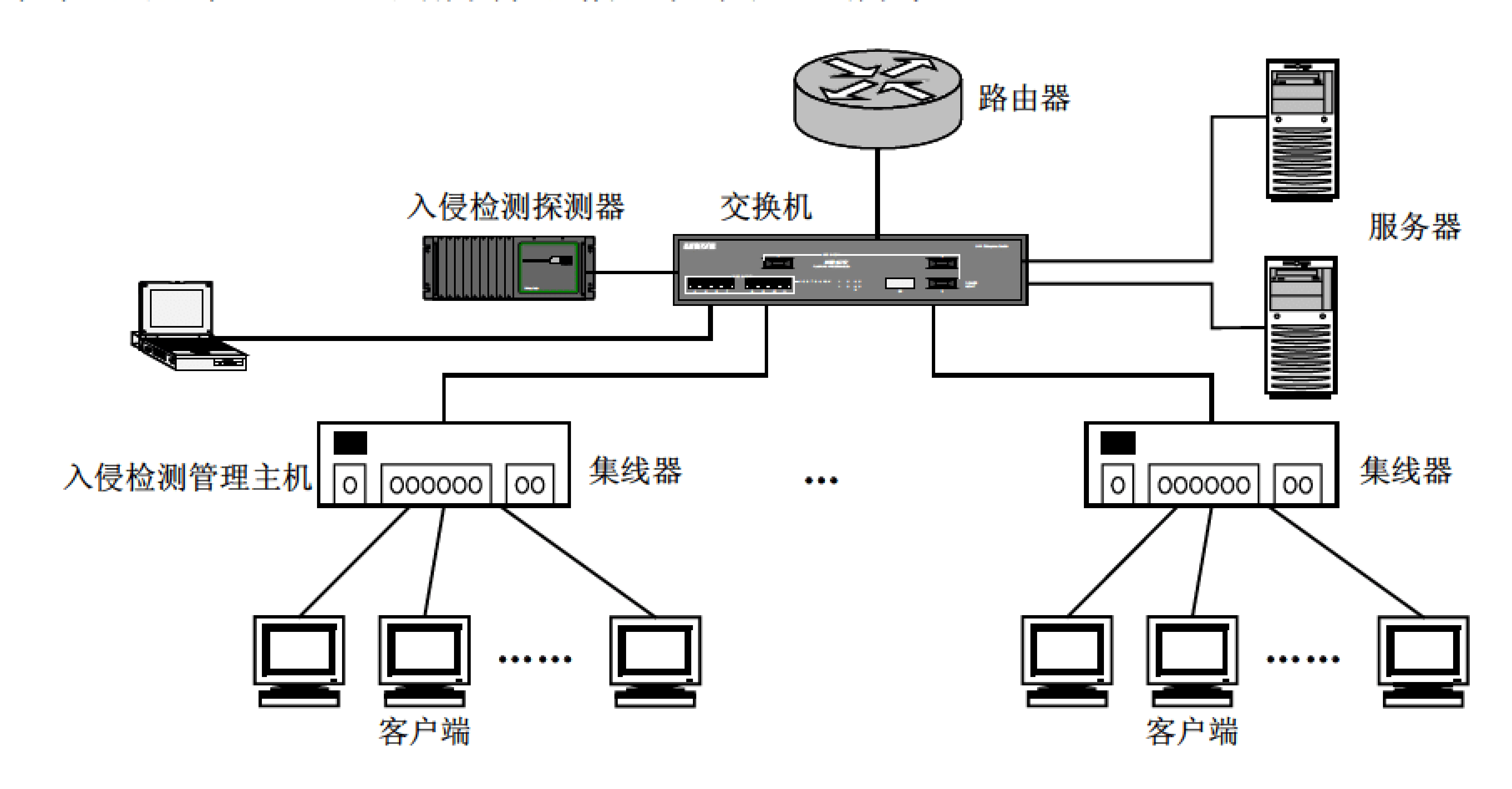


图 3-4　小规模网络环境应用

2)　分布式监测应用示例

网络结构相对较复杂，内部网络中各机构间使用交换机连接到主交换机上，通过主交换机连接路由器接入 Internet。此时，在主交换机的广播口(监听口)上无法监听到从交换机上的机器间的通信，为了全面监控网络，捕捉内部网间的恶意攻击与入侵行为，就需要为每个重要的网段部署一个入侵检测探测器，并分别将检测到的事件发送到集中管理控制台，如图 3-5 所示。

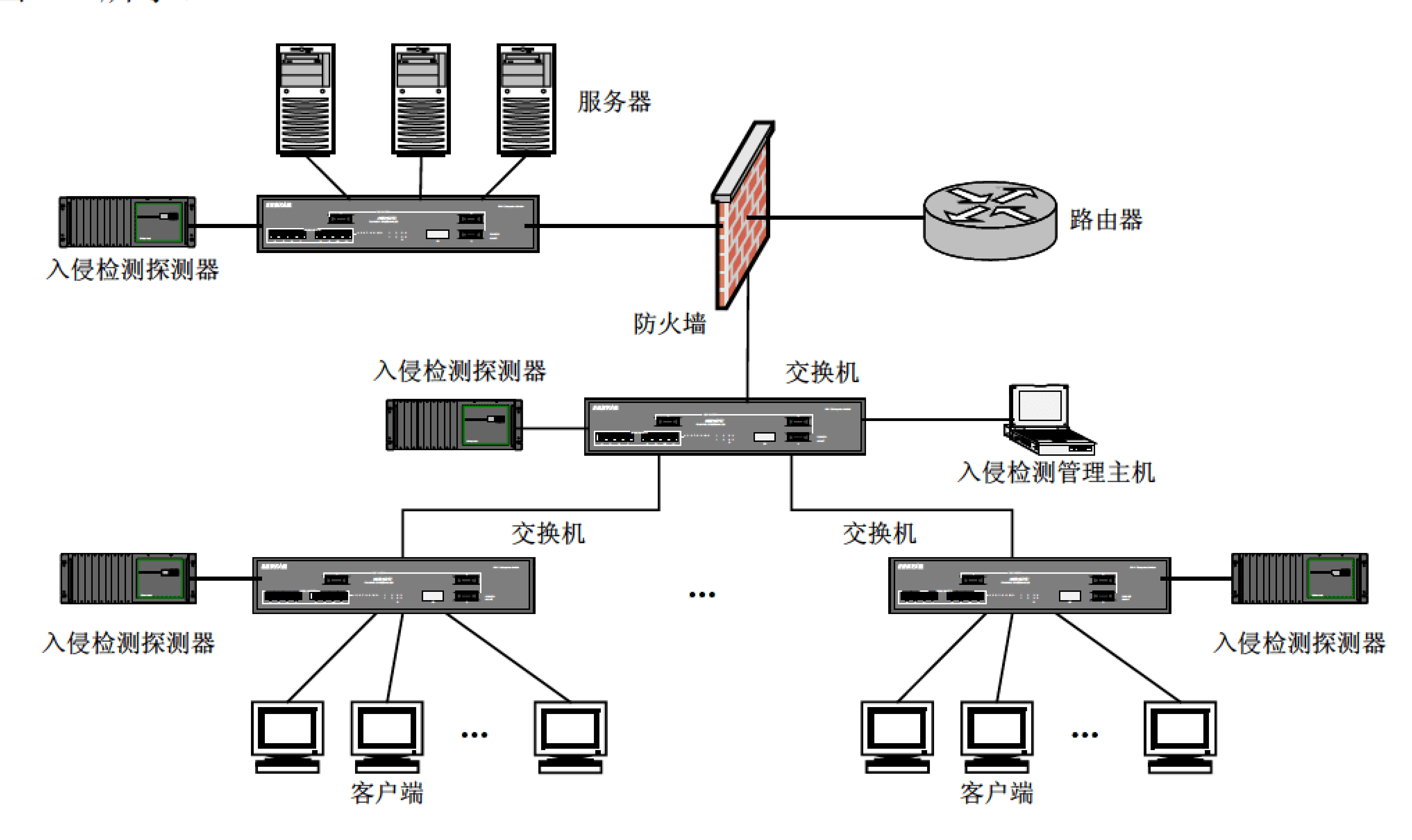


图 3-5　多子网分布式环境应用

3.1.2　典型例题分析

例 1　阅读以下说明，回答问题 1～问题 6，将解答填入答题纸对应的解答栏内。(2006 年 11 月下午试题四)

【说明】

特洛伊木马是一种基于客户机/服务器模式的远程控制程序，黑客可以利用木马程序入侵用户的计算机系统。木马的工作模式如图 3-6 所示。

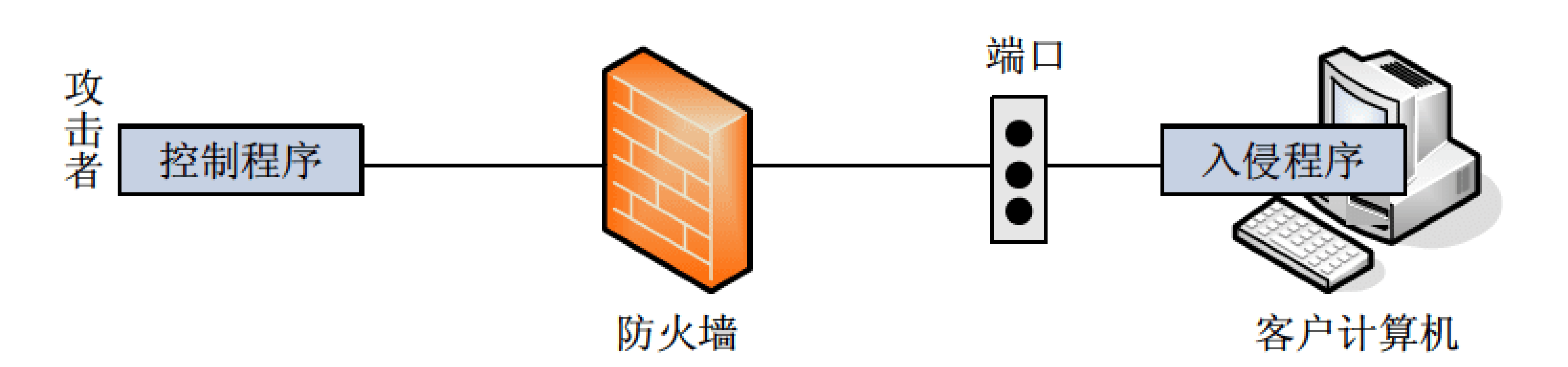


图 3-6　木马工作原理示意

【问题 1】(2 分)

对于传统的木马程序，侵入被攻击主机的入侵程序属于__(1)__。攻击者一旦获取入侵程序的__(2)__，便与它连接起来。

(1) A. 客户程序　B. 服务程序　C. 代理程序　D. 系统程序

(2) A. 用户名和口令　B. 密钥　C. 访问权限　D. 地址和端口号

【问题 2】(2 分)

以下 (3) 和 (4) 属于计算机感染特洛伊木马后的典型现象。

A. 程序堆栈溢出　B. 有未知程序试图建立网络连接

C. 邮箱被莫名邮件填满　D. 系统中有可疑的进程在运行

【问题 3】(2 分)

为了检测系统是否有木马侵入，可以使用 Windows 操作系统的 (5) 命令查看当前的活动连接端口。

A. ipport　B. netstat-an　C. tracert-an　D. ipconfig

【问题 4】(4 分)

入侵程序可以通过修改 Windows 操作系统的 (6) 、 (7) 文件或修改系统中的相关注册表项实现系统启动时自动加载。通过运行 Windows 操作系统中的 (8) (填空)命令，可以启动注册表编辑器来对注册表进行维护。

A. system.ini　B. shell.ini　C. win.ini　D. autoexec.ini

【问题 5】(2 分)

安装了防火墙软件的主机可以利用防火墙的 (8) 功能有效地防止外部非法连接来拦截木马。

A. 身份认证　B. 地址转换　C. 日志记录　D. 包过滤

【问题 6】(3 分)

以下措施中能有效防止木马入侵的有 (10) 和 (11) 。

A. 不随意下载来历不明的软件

B. 仅开放非系统端口

C. 实行加密数据传输

D. 运行实时网络连接监控系统

分析：

【问题 1】

特洛伊木马是一种基于客户端/服务器模式的远程控制程序，它可以让用户的机器运行服务器端的程序，该程序会在用户的计算机上打开监听的端口。这样就给黑客入侵用户计算机打开了一扇进出的门，黑客就可以利用木马程序的客户端入侵用户的计算机系统。因此，对于传统的木马程序，侵入被攻击主机的入侵程序属于服务器端程序，而攻击者掌握的是客户端程序，攻击者要想与入侵程序连接起来，需要得到入侵程序的地址和端口号。

【问题 2】

用户的计算机感染特洛伊木马后，会受到木马程序的控制，典型的现象有以下几种。

① 死机、重启，长时间读写硬盘、搜索软盘。

② 运行速度越来越慢，资源占用多。

③ 任务表中有可疑的文件在运行。

【问题 3】

当前最为常见的木马程序通常是基于 TCP/UDP 协议进行 Client 端与 Server 端之间通信

的，因此，可以通过查看在本机上开放的端口，来判断是否有可疑的程序打开了某个可疑的端口。查看端口的方法有以下几种。

- 使用 Windows 本身自带的 netstat 命令。例如：

```
C:\>netstat -an
```

- 使用 Windows 2000 下的命令行工具 fport，例如：

```
E:\software>Fport.exe
```

- 使用图形化界面工具 Active Ports。该工具可以监视到计算机所有打开的 TCP/IP/UDP 端口，还可以显示所有端口对应的程序所在的路径，本地 IP 和远端 IP 是否正在活动。这个工具适用于 Windows NT/2000/XP 平台。

【问题 4】

基于 Windows 的木马程序一般采用启动时自动加载应用程序的方法。其主要包括两种方法：一是修改 win.ini 和 system.ini 系统配置文件；二是修改注册表项。

【问题 5】

随着防火墙技术的提高和发展，基于 IP 包过滤规则来拦截木马程序可以有效地防止外部连接，因此黑客在无法取得连接的情况下，也无所作为。

【问题 6】

随着网路的广泛应用，硬件和软件的高速发展，网络安全显得日益重要。对于网络中比较流行的木马程序，传播时间比较快，影响比较严重，因此对于木马程序的防范就更不能疏忽。用户在检测清除木马程序的同时，还要注意对木马程序的预防，做到防患于未然。

具体应做到以下几点。

① 不要随意打开来历不明的邮件。
② 不要随意下载来历不明的软件。
③ 及时修补漏洞和关闭可疑的端口。
④ 尽量少用共享文件夹。
⑤ 运行实时监控程序。
⑥ 经常升级系统和更新病毒库。

答案：

【问题 1】

(1) B
(2) D

【问题 2】

(3) B
(4) D

说明：(3)、(4)可以互换。

【问题 3】

(5) B

【问题4】

(6) A

(7) C

说明：(6)、(7)可以互换。

(8) regedit

【问题5】

(9) D

【问题6】

(10) A

(11) D

说明：(10)、(11)可以互换

3.1.3 同步练习

1. 简述网络病毒防护策略。
2. 简述网络防病毒的组织形式。
3. 简述硬件防病毒网关的特色(与客户端、服务器软件类防毒产品相比)。
4. 简述网络病毒的特点。
5. 为了防范 Internet 的病毒对企业内部网的威胁，企业内部可购置什么防护系统？此系统应部署在什么地方？

3.1.4 同步练习参考答案

1、2、3、4 题答案见本节考点辅导。

5. 为了防范因特网的病毒对企业内部网的威胁，企业内部可购置防病毒过滤网关防护系统。此系统部署在用户内部网与外部网的接入点处。

3.2 防火墙的配置策略和漏洞处理策略

3.2.1 考点辅导

3.2.1.1 防火墙概述

1. 什么是防火墙

防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合。它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，来防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。

2. 防火墙的相关概念

防火墙的相关概念有：非信任网络(公共网络)、信任网络(内部网络)、DMZ(非军事化区)、可信主机、非可信主机、公网 IP 地址、保留 IP 地址、包过滤、地址转换。

- 非信任网络(公共网络)：处于防火墙之外的公共开放网络，一般指 Internet。
- 信任网络(内部网络)：位于防火墙之内的可信网络，是防火墙要保护的目标。
- DMZ(非军事化区)：也称周边网络，可以位于防火墙之外，也可以位于防火墙之内。安全敏感度和保护强度较低。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问，所以无法提供与内部网主机相等的安全性。
- 可信主机：位于内部网的主机，且具有可信任的安全特性。
- 非可信主机：不具有可信特性的主机。
- 公网 IP 地址：由 Internet 信息中心统一管理分配的 IP 地址，可在 Internet 上使用。
- 保留 IP 地址：专门保留用于内部网的 IP 地址。可以由网络管理员任意指派，在 Internet 上不可识别和不可路由，如 192.168.0.0 和 10.0.0.0 等地址网段。
- 包过滤：防火墙对每个数据包进行允许或拒绝的决定。具体地说，就是根据数据包的头部按照规则进行判断，决定继续转发还是丢弃。
- 地址转换：防火墙将内部网主机不可路由的保留地址转换成公共网络可识别的公共地址，可以达到节省 IP 和隐藏内部网络拓扑结构信息等目的。

3. 防火墙的特性

防火墙的功能及优点如下。

- 对进出的数据包进行过滤，过滤掉不安全的服务和非法用户。
- 监视 Internet 安全，对网络攻击行为进行检测和报警。
- 记录通过防火墙的信息内容和活动。
- 控制对特殊站点的访问，封堵某些禁止的访问行为。
- 防火墙能强化安全策略，执行系统规定的规则，仅允许符合规则的信息通过。
- 防火墙能有效地记录 Internet 上的活动。因为所有进出的信息都需要经过防火墙，所以防火墙可以记录信任网络和非信任网络之间发生的各种事件。
- 防火墙是一个安全策略的边防站。因为所有进出内部网的信息都必须通过防火墙，所以防火墙便成为一个安全检查站，能够把可疑的连接或者访问拒之门外。

防火墙具有以下缺点。

- 防火墙不能防范不经过防火墙的攻击。未经过防火墙的数据，防火墙无法检查，比如拨号上网。
- 防火墙不能解决来自内部网络的攻击和安全问题。对于防火墙内部各主机间的攻击行为，防火墙就爱莫能助。
- 防火墙不能防止最新的未设置策略或错误配置引起的安全威胁。因为防火墙的各种策略是在某攻击方式经过专家分析后给出其特征而设置的。
- 防火墙不能防止人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。
- 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议而实

现的，因此就无法解决 TCP/IP 操作的漏洞。比如，DoS 或 DDoS 攻击。

- 防火墙对服务器合法开放的端口的攻击大多无法阻止。
- 防火墙不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。
- 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。
- 防火墙不能防止内部的泄密行为。对于内部的一个合法用户主动泄密，防火墙是无能为力的。
- 防火墙不能防止对本身安全漏洞的威胁。防火墙保护别人有时却无法保护自己，因为目前还没有厂商绝对保证防火墙不会存在安全漏洞。防火墙也有一个操作系统，也有着其硬件系统和软件，因此依然有着漏洞和 Bug，所以其本身也可能受到攻击和出现软件和硬件方面的故障。

4. 防火墙的基本分类

根据防火墙实现原理的不同，通常将防火墙分为包过滤防火墙、应用层网关防火墙和状态检测防火墙 3 类。

3.2.1.2 防火墙系统的安装与配置

下面主要以方正方御防火墙为例对防火墙的安装和配置进行说明。

1. 软硬件安装

方御防火墙的软件部分主要由管理监控程序(FireControl)、串口配置程序(FCInit)和日志报警程序(LogService)组成。FireControl 是方御防火墙的管理程序，其作用是管理、监控、配置防火墙和设置入侵攻击报警策略，进行设备管理和日常监控；FCInit 的主要功能是初始化 FG 防火墙，它通过配置串口来完成初始化工作；LogService 的功能是获取日志、提供日志报警信息，在程序的安装过程中，能够自动装载数据和文件，并在系统程序组中，生成方御防火墙的程序组。

方御防火墙的硬件名称为 FireGate，简称 FG。其硬件安装步骤如下。

(1) 用网线将外部网接口连接到 FG 的外部接口。
(2) 用网线将内部网接口连接到 FG 的内部接口。
(3) 用网线将控制主机连接到 FG 的控制接口。
(4) 用网线将开放区服务器接到 DMZ 区接口。
(5) 用电源线将 FG 接上电源，硬件安装完成。

其硬件安装结构如图 3-7 所示。

2. 基本配置

FireControl 安装在控制机上，控制机可以是与 FireControl 网口相连的任意台机器；在 FireControl 安装程序完毕后，即可在桌面上找到它的快捷方式。

管理员第一次启动 FireControl 管理程序时，应使用在 FCInit 中新建实施域时创建的默认帐号 admin 进行登录。登录成功后，为安全起见，建议即刻修改 admin 帐号的密码，以策略管理员身份登录 FireControl。策略管理员可自定义防火墙的各种参数，配置个性化的防

火墙。防火墙的基本配置包括以下几个方面。

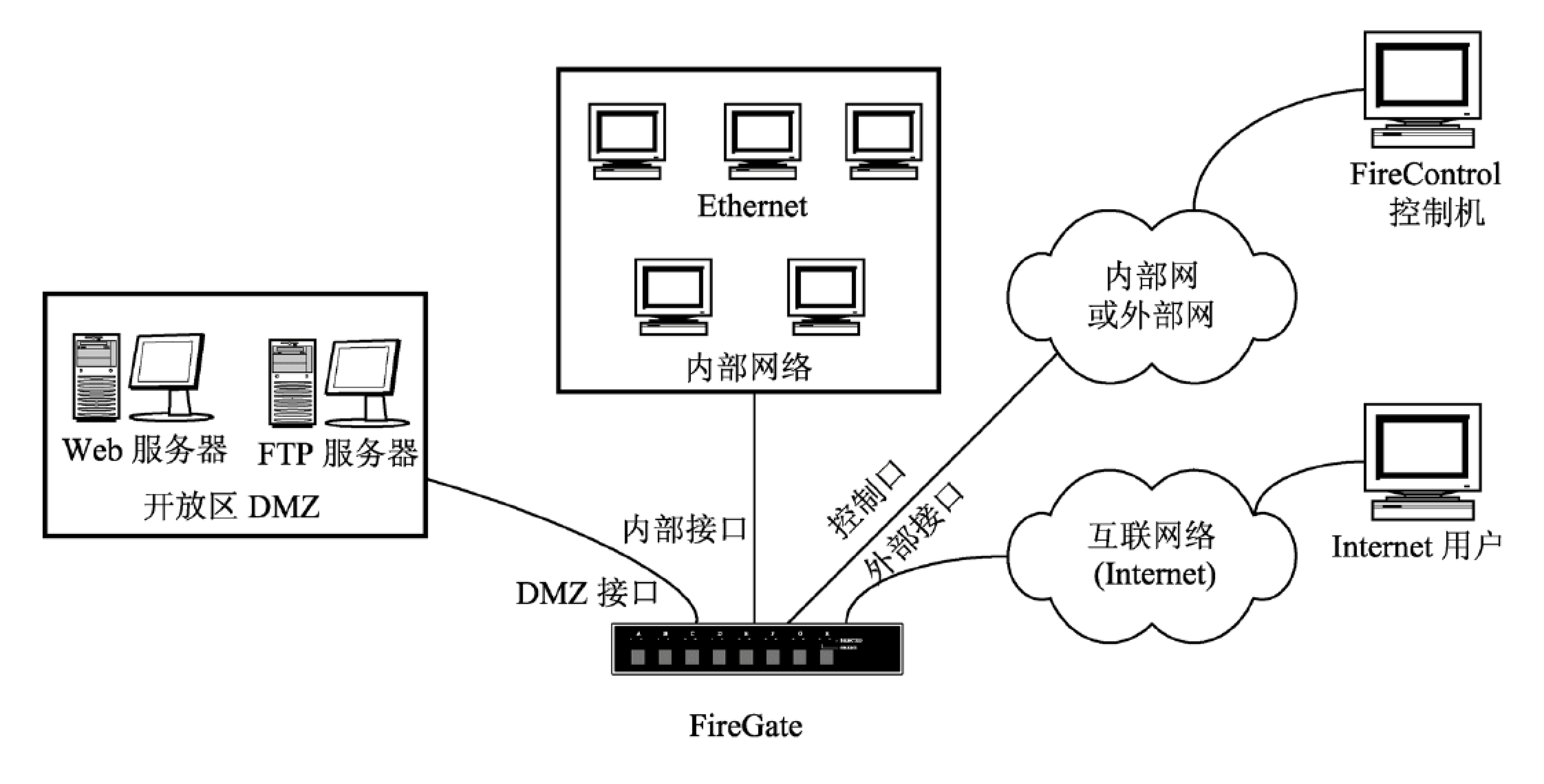


图 3-7　硬件安装结构

1)　别名

别名配置是指为相关网络地址和端口设置别名。别名的设计是为了方便策略管理员的使用。策略管理员可以使用好记的别名代替多个功能端口以及子网，使配置不再烦琐。例如，使用别名 www 代替端口 80 或 8080，别名 office 代替 IP 地址为 105.118.0.0、子网掩码为 255.255.255.0 的网段地址，或者把几个离散的端口值和网段地址统一用一个别名进行管理。

别名是 FG 防火墙中重要的特性，大部分防火墙规则的配置都是通过别名来实现的，策略管理员在配置安全规则时需要先定义好相关的网络地址和端口的别名。

2)　设备配置

设备配置是防火墙自身的网络设置，包括对接口设备的配置和显示防火墙的基本信息。在 FG 初始化完成，以策略管理员身份登录后，首先需要进行设备配置，用户可以根据自己实际的网络需求在设备配置模块中通过对网络接口的设置实现多种工作模式。

防火墙可以有 3 种工作模式：桥模式、路由模式和混杂模式。

- 桥模式：如果用户不想改变原有的网络拓扑结构和设置，可以将防火墙设置成桥模式。在桥模式下，网络间的访问是透明的，所有网口设备将构成一个网桥。
- 路由模式：是防火墙的基本工作模式。在路由模式下，防火墙的各个网口设备的 IP 地址都位于不同的网段。
- 混杂模式：指防火墙部分网口在路由模式下工作，部分网口在桥模式下工作。即某些子网之间以路由方式通信，而某些子网之间可以透明通信。

3)　SNMP 配置

FG 支持 SNMP 简单网络管理协议。一方面，网络管理工具可以实时获取 FG 的状态，为其提供相关的系统状态、网络接口状态、IP 状态、ARP 表状态和 SNMP 服务状态等信息；另一方面，FG 为网络管理平台定期提供有关 FG 防火墙的信息，如入侵信息、管理信息和

系统信息。

SNMP 的界面配置可分为以下 4 个部分。

- 防火墙位置标识：对系统本地位置信息进行配置。
- 共同体(Community)：用于简单的权限控制，默认为 public。
- SNMP 管理服务器地址：网络管理服务器地址。
- 管理服务器 Trap 服务端口：网络管理服务器 Trap 接收端口，默认为 162。

4) 双机热备份技术

双机热备份是指一台 FG 为主机，正常情况下处于工作状态，另一台 FG 作为备用机，平时处于备用状态，并不工作，当工作状态的系统出现故障时，备用状态的防火墙在保证网络正常使用的情况下，可立即自动切换到工作状态，接替主机的角色，承担防火墙的工作。

方御防火墙系统在桥模式下能够在网络中智能地寻找其对等的备份机，并且使备份机自动进入等待状态，而一旦备份机发现主工作机失效，可及时地启动，防止网络中断事故的发生。要保护网络的安全，防火墙本身首先要安全。即使防火墙未被黑客攻击，也会由于元器件老化、异常死机等特殊原因发生故障。一旦发生故障，网络的安全就无法保证。对可靠性要求很高的用户，一定要选用有双机热备份技术的防火墙。FG 在路由模式下的双机热备份需要手工设置。

双机热备份连接如图 3-8 所示，G 的 COM 2 口需要用串口线连接；两台 FG 的内部、外部、DMZ 区以及控制接口需要分别通过交换机或集线器用网线连接。硬件连接完成后，需要在 FG 控制端进行设置。只有策略管理员可以设置双机热备功能。双机热备份系统只在桥模式和路由模式下工作，不支持混杂模式及 VLAN。

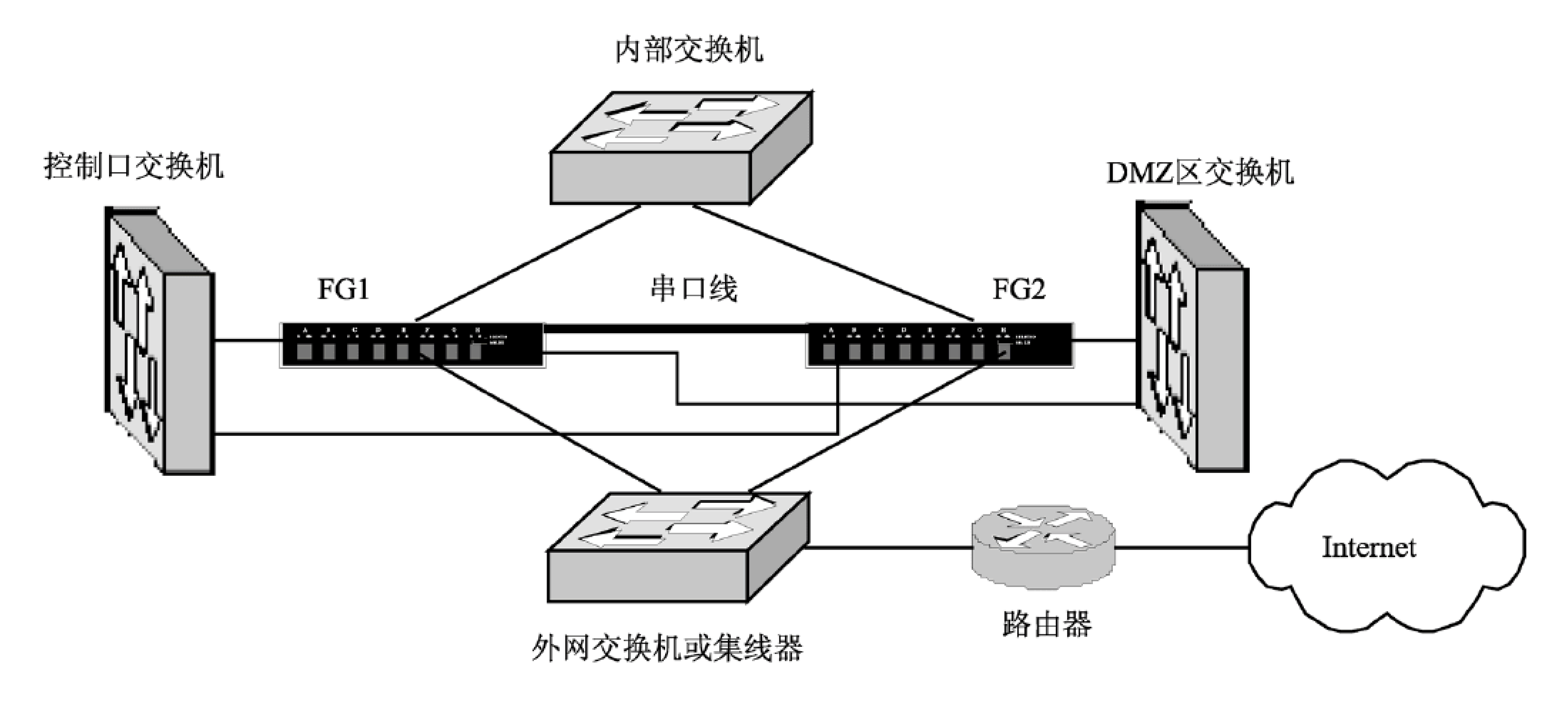


图 3-8 双机热备份连接示意

3. 规则配置

FG 防火墙提供基于状态检测技术的包过滤，能够根据数据包的地址、协议和端口进行访问控制。FG 防火墙包过滤功能主要是通过制定过滤规则集，对数据包头源地址、目的地址和端口号、协议类型等标志进行检查，以判定是否允许通过。对于满足过滤规则的数据

包，可以选择放过或者丢弃，不满足规则的包则被丢弃。包过滤规则采用按顺序匹配的方式，即首先匹配前面的规则，若匹配则不再向下执行，因此一定要注意规则设置的顺序问题。

防火墙的规则配置是面向网口设备的，每个网口上的规则是指：每个接口设备接收到的数据包要经过这些规则的过滤，此处的接口包括物理接口设备和 VLAN 设备。每条规则详细描述了源/目的地址、目的端口、协议、数据流向、状态检测和策略等信息。

策略包括 4 种：禁止(DROP)、允许(ACCEPT)、用户认证(AUTH)和自动封禁(AUTO)。

- 允许：接收此包。
- 禁止：丢弃此包。
- 用户认证：对于分配了公网 IP 的内部用户，如果出于安全性考虑目的，管理员希望用户必须通过认证才能访问因特网，则需要在用户管理模块中选择一种认证方式(内置帐号认证或第三方认证)，并且在防火墙模块的相应接口设备上(一般是内部网对应的网口)添加一条用户认证规则。
- 自动封禁：FG 启动入侵检测功能后，需要在防火墙模块相应接口设备(包括物理网口、VLAN 设备)上添加一条“自动封禁”规则，才能自动封禁入侵 IP。FG 的每个网口都可以自动封禁。一般情况下，要设置入侵检测功能的自动封禁，选择物理网口进行监听。

3.2.1.3　访问控制列表

1. 基本概念

(1)　IP 包过滤技术：路由器在转发数据包时，先获取包头信息(包括 IP 层所承载的上层协议的协议号，数据包的源地址、目的地址、源端口号和目的端口号等)，然后与设定的规则进行比较，再根据比较的结果对数据包进行转发或者丢弃。

(2)　IP 访问控制列表是实现包过滤的核心技术。访问控制列表就是一系列允许和拒绝条件的集合，通过访问列表可以过滤发进和发出的信息包的请求，实现对路由器和网络的安全控制。路由器逐个地检测包与访问列表的条件，在满足第一个匹配条件后，就可以决定是否接收或拒收该包。

2. 访问控制列表的分类和配置

1)　IP 访问控制列表的分类

- 标准访问列表：只对数据包中的源地址进行检查，而不考虑目的地址及端口号等过滤选项，表号为 1～99。
- 扩展访问列表：既检查包的源地址，也检查包的目的地址，还可以检查特殊的协议类型、端口以及其他参数，具有更大的自由度，表号为 100～199。

2)　IP 访问控制列表的配置

(1)　配置步骤。

①　在全局配置模式下，创建 ACL。

```
Router(config)#access-list access-list-number {permit | deny }
{test-conditions}
```

② 在接口配置模式下，使用 access-group 命令将 ACL 应用到某一接口上。

```
Router(config-if)#ip access-group access-list-number {in | out }
```

其中，in 和 out 参数可以控制接口中不同方向的数据包，如果不配置该参数，默认为 out。

(2) 创建访问控制列表。

- 通配符掩码：在创建访问控制列表，表示一定范围的 IP 地址时，不使用子网掩码而使用通配符掩码。通配符掩码可用 255.255.255.255 减去子网掩码求出。
- 在通配符掩码中，可以用 255.255.255.255 表示所有 IP 地址，也可以用 any 来取代。而 0.0.0.0 的通配符掩码则表示所有 32 位都要进行匹配，这样只表示一个 IP 地址，可以用 host 来表示。

① 创建标准访问控制列表。

```
Router(config)# access-list access-list-number {deny | permit}
                source  [source-wildcard ]
```

参数说明：access-list-number 是定义访问列表的编号，取值范围为 1～99；deny 或 permit 指定了允许还是拒绝数据包；source 是发送数据包的主机地址；source-wildcard 是发送数据包的主机的通配符掩码。

② 创建扩展访问控制列表。

```
Router(config)#access-list access-list-number {permit | deny}
    protocol {source [source-wildward] |any }
    {destination [destination-wildcard] |any }
    [protocol-specific options] [established] [log]
```

参数说明如下。

- access-list-number：定义访问列表的编号，取值范围为 100～199。
- deny 或 permit：指定了允许还是拒绝数据包。
- protocol：协议，如 IP、TCP、UPD、ICMP、OSPF 等。
- source、destination、destination-wildcard：源地址和目标地址。
- source-wildcard：通配符掩码。
- protocol-specific options：指定协议选项，用 lt、eq、gt、neq(小于、等于、大于、不等于)加端口号来指定，如 eq 80。

3.2.1.4 配置 Cisco PIX 防火墙

(1) 配置方法：基本上与路由器、交换机的相同，包括初始配置必须使用控制台端口(Console)方式，同时支持 Telnet、FTP 服务器等配置方式。

(2) 常用的配置命令：有 nameif、interface、ip address、nat、global、route、conduit、telnet、write memory 等。

- 配置防火墙接口的名字，并指定安全级别(nameif)：

  ```
  Firewall(config)#nameif hardware_id interface security_level
  ```

  在默认配置中，以太网口 0 被命名为外部接口(Outside)，安全级别是 0；以太网口 1 被命名为内部接口(Inside)，安全级别是 100。安全级别取值范围为 1～99，数字

越大安全级别越高。

- 配置网络接口参数(interface)：配置接口的参数，如双工、速率、启用或停用。

```
Firewall(config)#interface hardware_id [hardware_speed] [shutdown]
```

- 配置内外网卡的 IP 地址(ip address)：ip address 用于手动配置一个接口上的 IP 地址，将一个逻辑地址添加到一个硬件 ID 上。

```
Firewall(config)#ip address if_name ip_address [netmask]
```

- 指定外部地址范围(global)：把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。

```
Firewall(config)#global (if_name) nat_id ip_address-ip_address
    [netmask global_mask]
```

- 配置地址轮换(nat)：将内网的私有 IP 转换为外网的公有 IP。Nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

```
Firewall(config)#nat (if_name) nat_id local_ip [netmask]
```

- 设置指向内网和外网的静态路由(route)：route 告诉我们要在哪个特定的网口转发，并指定哪个网络地址。

```
Firewall(config)#route (if_name) 0 0 gateway_ip [metric]
```

- 设置某些控制选项(conduit)：用于允许数据包从较低安全级别流向较高安全级别。通常是外网对内网的访问。

```
Firewall(config)#conduit global_ip port[-port] protocol
    foreign_ip [netmask]
```

- 设置 telnet 选项(telnet)：在默然情况下，PIX 的以太端口是不允许 Telnet 的，配置只能通过 Console 口，这一点与路由器有区别。可以通过 telnet 命令指定哪些计算机能够用 telnet 登录到防火墙。

```
Firewall(config)#telnet local_ip [netmask]
```

- 保存配置(write memory)：将运行的配置文件保存到 NVRAM 中。

```
Firewall(config)# write memory
```

- 测试命令如下。

```
Firewall(config)#ping                    (连通性测试)
Firewall(config)#show interface          (查看端口状态)
Firewall(config)#show static             (查看静态地址映射)
Firewall(config)#write terminal          (查看配置)
```

3.2.1.5 其他设置

1. 安全套接层(SSL)

(1) SSL：提供了两台计算机之间的安全连接，对整个会话进行了加密，从而保证了安全传输。工作在应用层和传输层之间，但属于传输层协议。

(2) SSL 的体系结构如图 3-9 所示。

HTTPS、FTPS、TELNETS、IMAPS 等			应用层
SSL 握手协议	SSL 修改密文协议	SSL 告警协议	SSL 层
SSL 记录协议			
TCP			传输层
IP			网络层

图 3-9 SSL 协议与 TCP/IP 协议间的关系

(3) SSL 的功能：具有三个基本功能，即验证身份、数据的机密性和报文的完整性。

(4) SSL 会话与 SSL 连接。

连接：是提供恰当类型服务的传输。对于 SSL，这样的连接是点对点的关系。连接是短暂的，每一个连接与一个会话相联系。

会话：SSL 的会话是客户与服务器之间的关联。会话通过握手协议来创建。

(5) SSL 握手过程。由 SSL 握手来完成，其过程如下。

① SSL 客户机连接至 SSL 服务器，并要求服务器验证其自身的身份。

② 服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个认证书颁发机构(CA)认证为止。通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性。

③ 服务器发出一个请求，对客户端的证书进行验证，但是由于缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

④ 协商用于加密的消息加密算法(如 IDEA、RC4、DES、3DES、RSA 等)和用于完整性检查的哈希函数(如 MD5、SHA 等)。通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。

(6) 数据封装：SSL 记录协议从高层接收到数据后要经过分段、压缩和加密处理，最后由传输层发送出去，从而保证了数据的机密性和报文的完整性。其数据的封装过程如下。

① 分片。将上层交付的报文分成 2^{14} 字节或更小的数据块。

② 可选地应用压缩。

③ 使用共享密钥计算报文鉴别代码(MAC)。

④ 使用同步算法加密报文。

⑤ 附加首部数据，包括内容类型、主要版本、次要版本及压缩长度。

⑥ 接收方接收到数据后，将其解密、验证、解压和重新装配，最后交回给高层用户。


2. 设置 IE 的 WWW 浏览环境

利用 IE 浏览因特网时，通常需要设置 WWW 的浏览环境。用户可以利用 IE 浏览器【工具】菜单下面的【Internet 选项】子菜单设置相应的浏览环境。

(1) 常规设置：可以设置主页、Internet 临时文件夹、历史记录，以及颜色、字体、语言和辅助工具等相关内容。

(2) 安全设置：用于设定或修改网络区域的安全级别。

(3) 隐私设置：是 IE 6.0 新加入的设置，主要包括隐私和弹出窗口设置。

(4) 内容设置：设置分组审查、证书和个人信息等。

(5) 连接设置：主要包括拨号和虚拟专用网设置以及局域网设置。

(6) 程序设置：用于指定 Windows 自动应用于 Internet 服务的程序。

(7) 高级设置：用于详细设定 IE 查看 Web 资源时的可选设置参数。

3.2.1.6　漏洞处理策略

漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的程序，是检测远程或本地系统安全脆弱性的一种安全技术。

1. 漏洞扫描工具

在网络安全策略的引导下，对网络可能存在的安全漏洞进行扫描，预先评估网络的安全性能，提供详细的网络安全隐患报告，找出网络的安全漏洞，给出网络漏洞修补建议是提高网络安全的重要措施，是保持网络安全的积极防御手段。网络漏洞扫描系统作为网络安全性的评估工具，一直受到网络安全产品提供商的重视，研发了具有不同特点的漏洞扫描工具。

漏洞扫描工具主要是静态对网络中的各种系统、设备和数据库进行漏洞扫描，找出整个网络系统中最容易受到攻击的地方，对网络进行有效的评估，最后提出建设性的解决方案。其工作原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象。漏洞扫描工具可以分为三种：基于服务器的扫描器、基于网络的扫描器和基于数据库的扫描器，分别可以对服务器、网络及数据库的安全漏洞进行扫描并提出安全分析报告。

2. 漏洞处理策略

漏洞形成的原因形形色色、不一而足，最常见的漏洞主要包含以下类型：CGI 脚本、POP3、FTP、SSH、HTTP、SMTP、IMAP、后门、RPC、DNS 漏洞等。根据不同的漏洞类型会有不同的漏洞处理策略。

3.2.2　典型例题分析

例 1　阅读以下说明，回答问题 1～问题 3，将解答填入答题纸对应的解答栏内。(2009 年 11 下午试题四)

【说明】

某公司通过服务器 S1 中的“路由和远程访问”服务接入 Internet，其拓扑结构如图 3-10 所示。其中，服务器 S1 的操作系统为 Windows Server 2003，公司从 ISP 处租用的公网 IP 地址是 202.134.135.88/29。

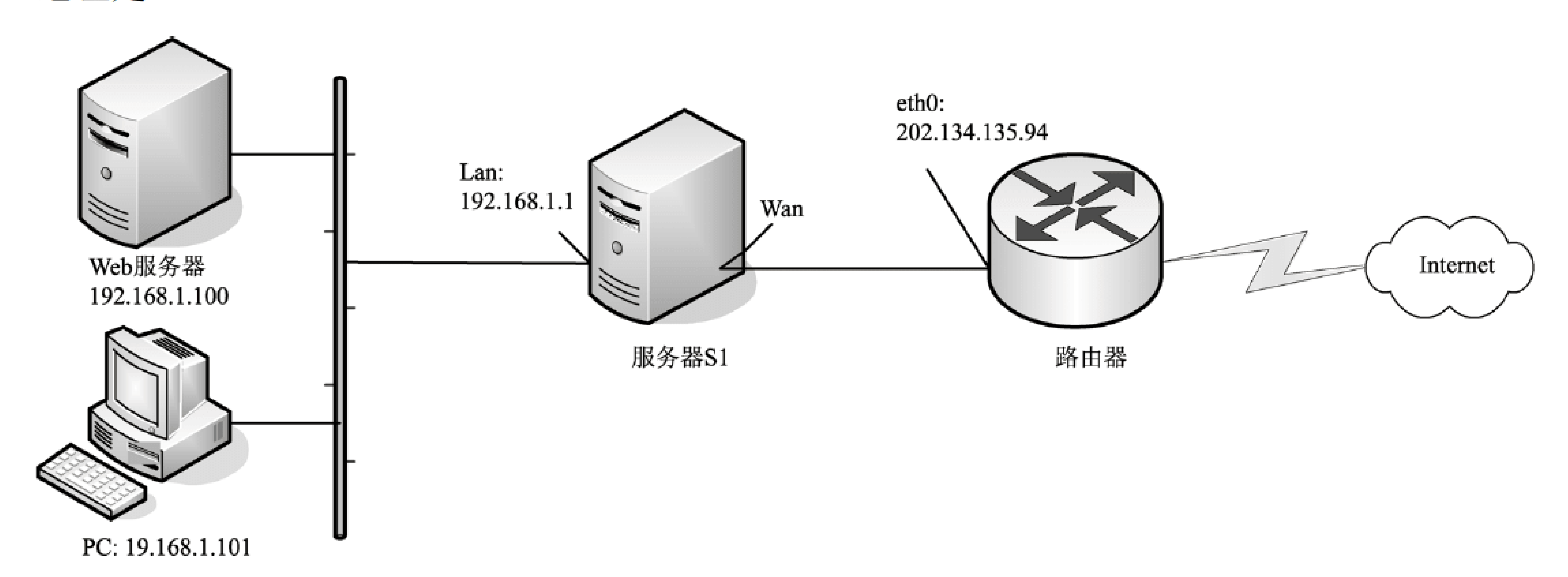
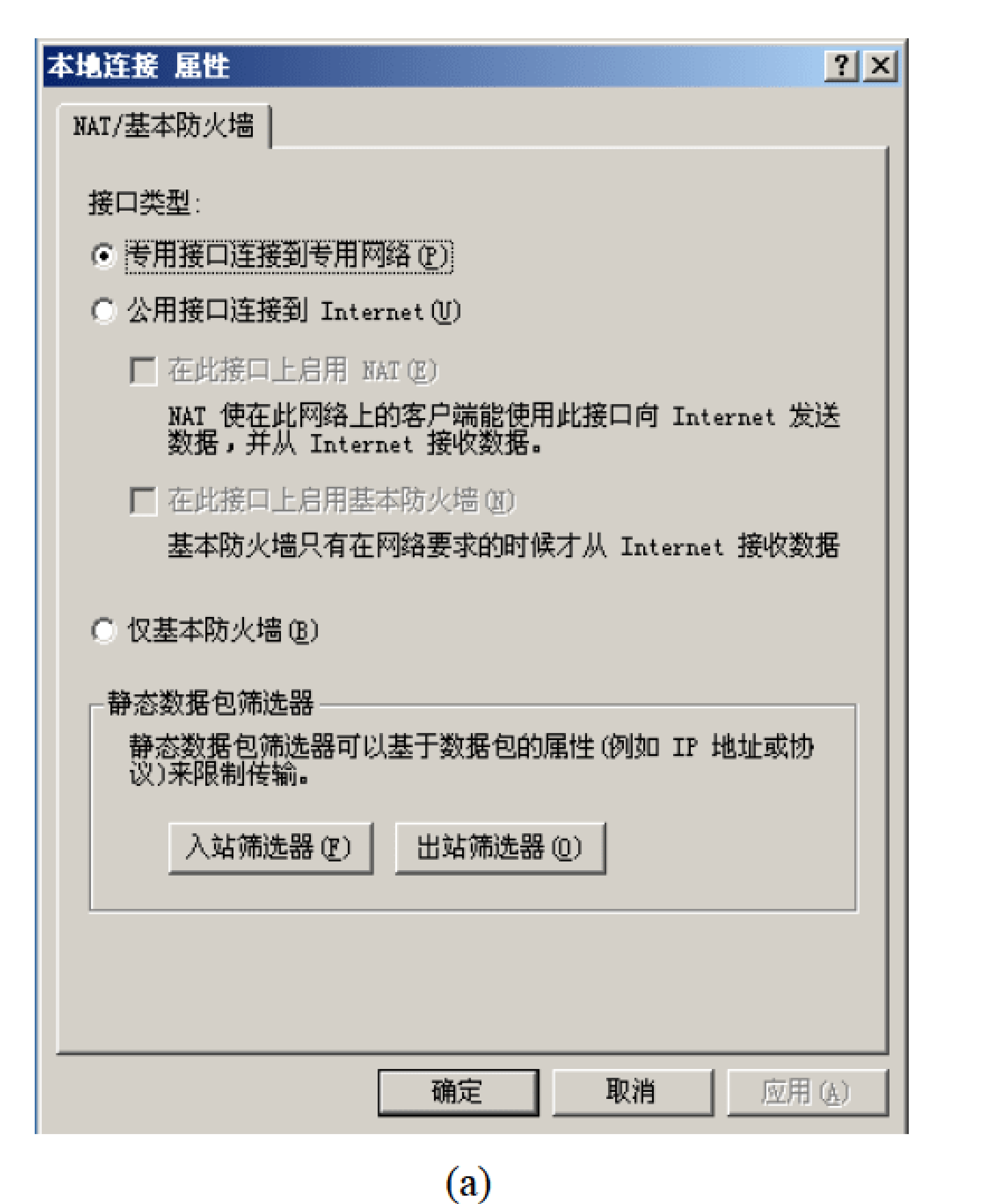


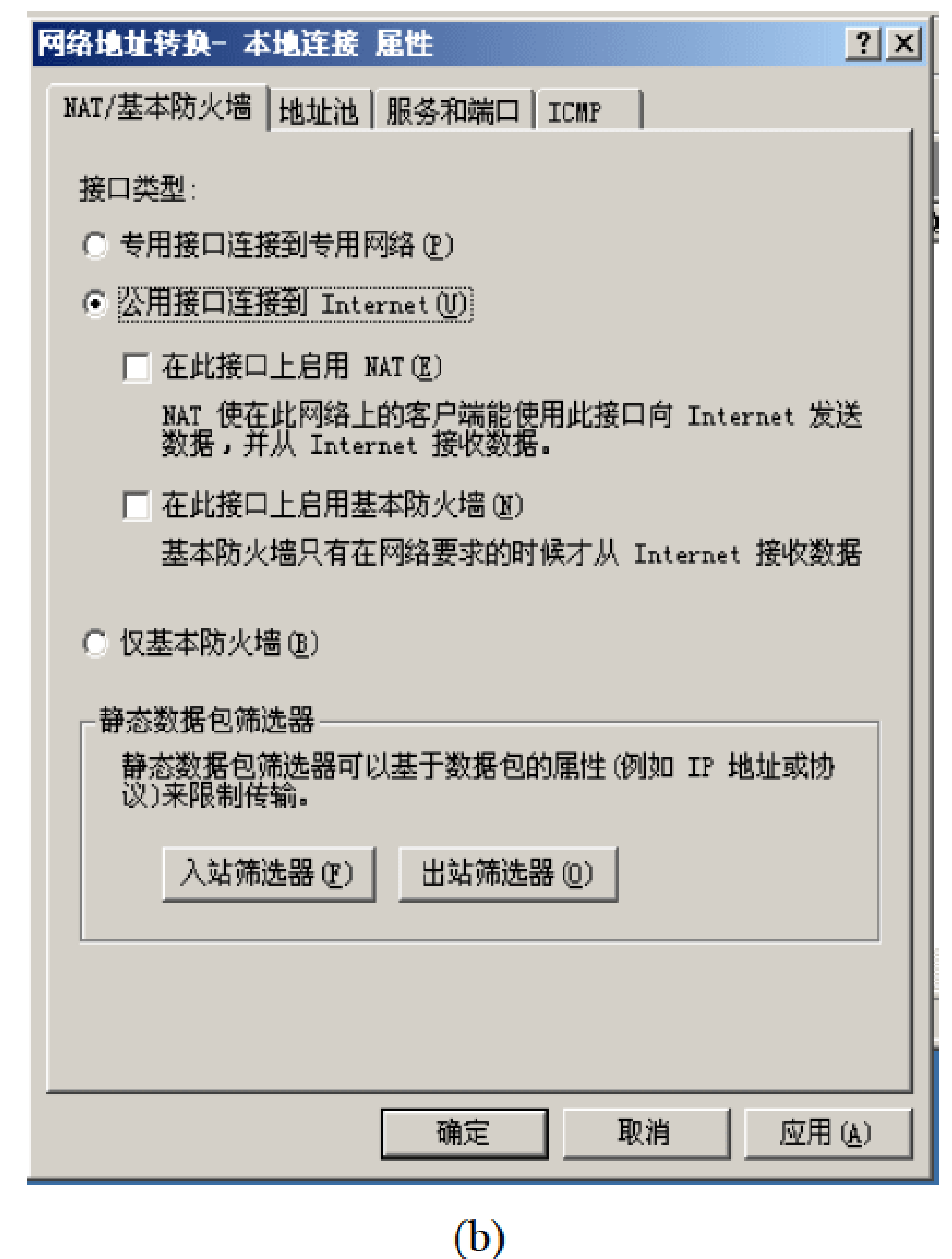
图 3-10　某公司网络拓扑结构

【问题 1】(4 分)

对服务器 S1 进行配置时，打开 NAT/基本防火墙配置对话框，在图 3-11(a)、(b)、(c)中，配置 Lan 接口的是__(1)__，配置 Wan 接口的是__(2)__。

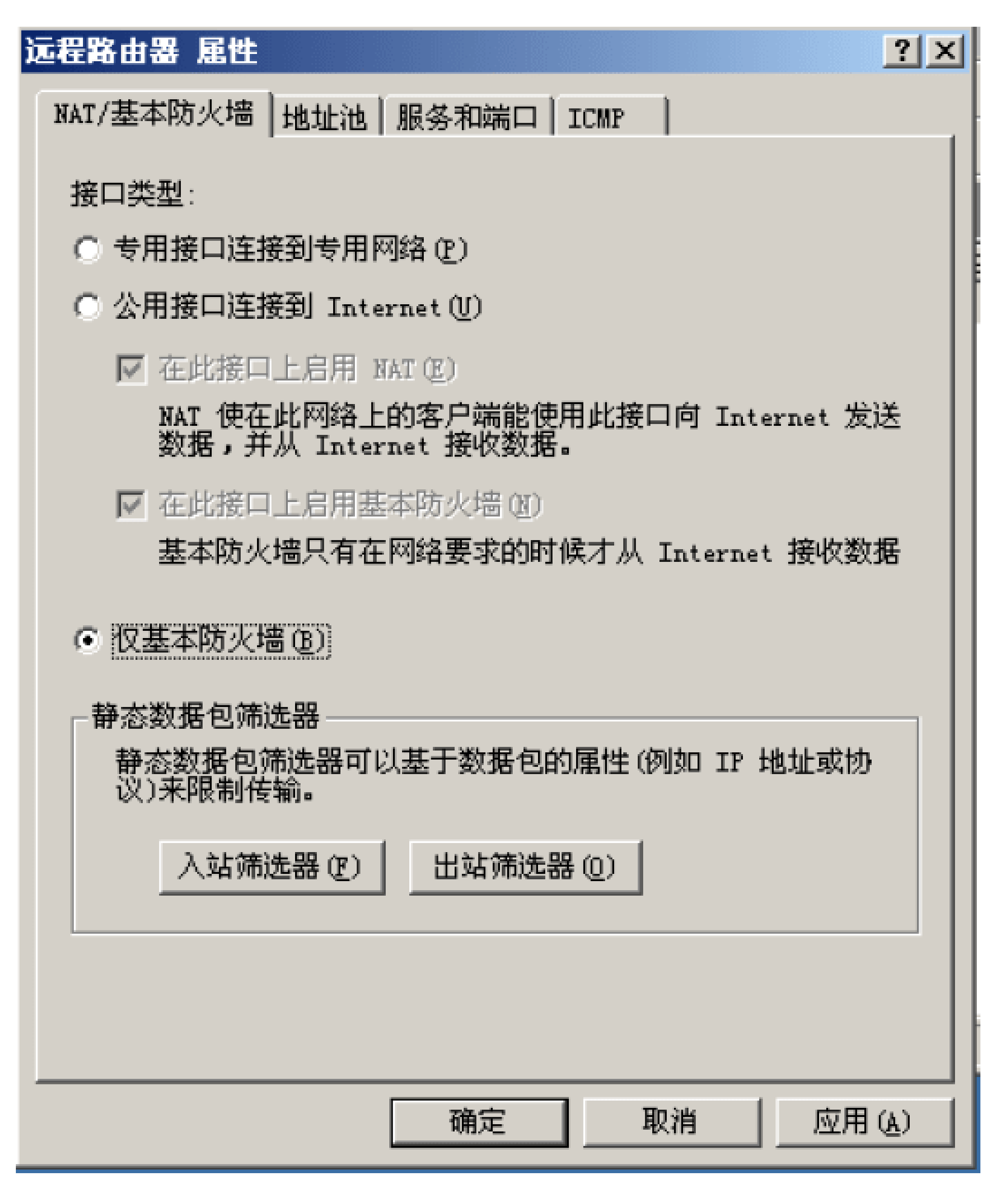


(a)



(b)

图 3-11　NAT/基本防火墙配置对话框



(c)

图 3-11　(续)

【问题 2】(8 分)

为保证内网 PC 可以访问 Internet，在图 3-12 所示的 Wan 接口的地址池中，起始地址为__(3)__，结束地址为__(4)__。

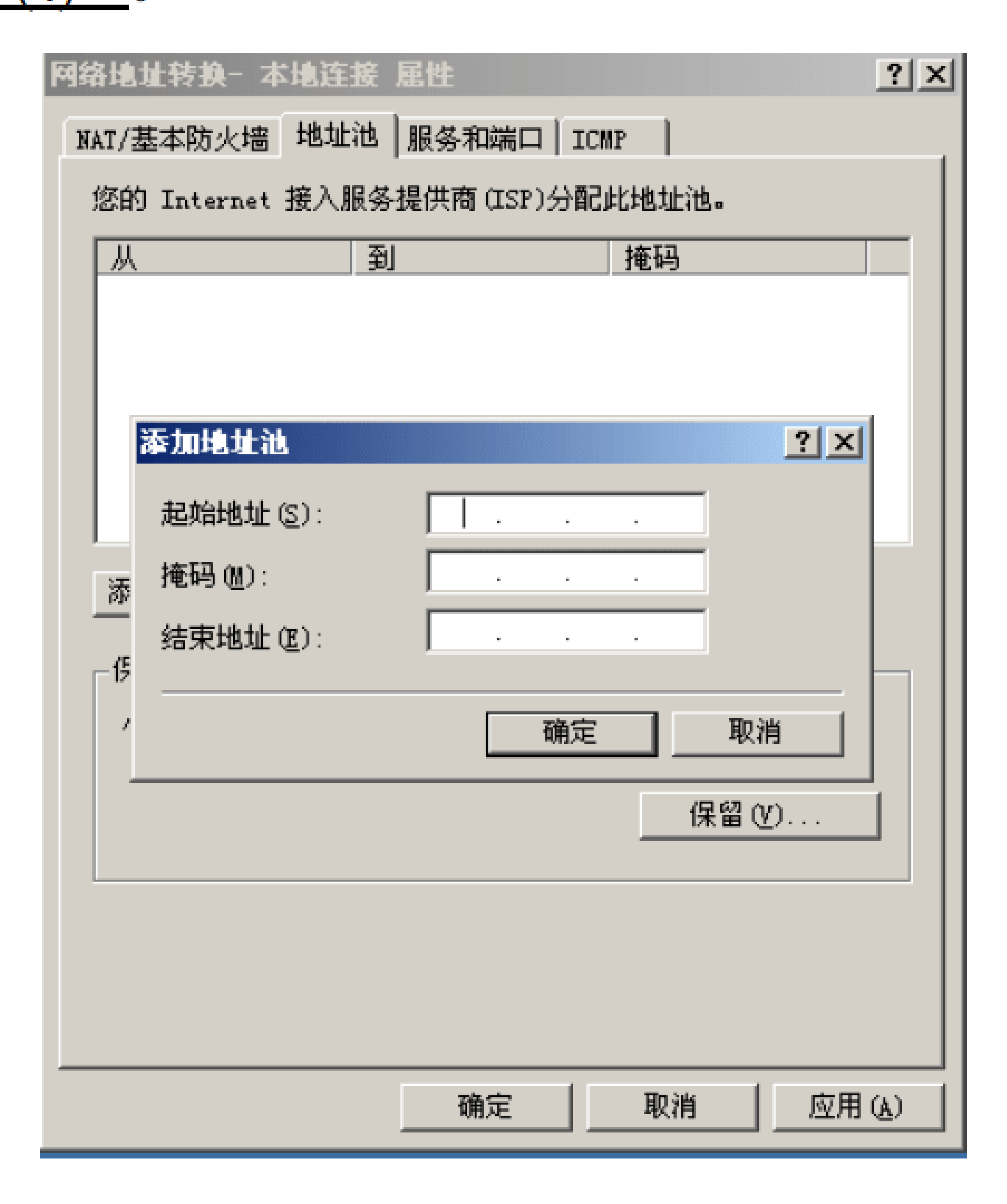


图 3-12　添加地址池

如果内网中 Web 服务器对外提供服务的 IP 地址是 202.134.135.92，则需要在图 3-13 中【保留此公用 IP 地址】文本框中填入 (5) ，【为专用网络上的计算机】文本框中填入 (6) 。

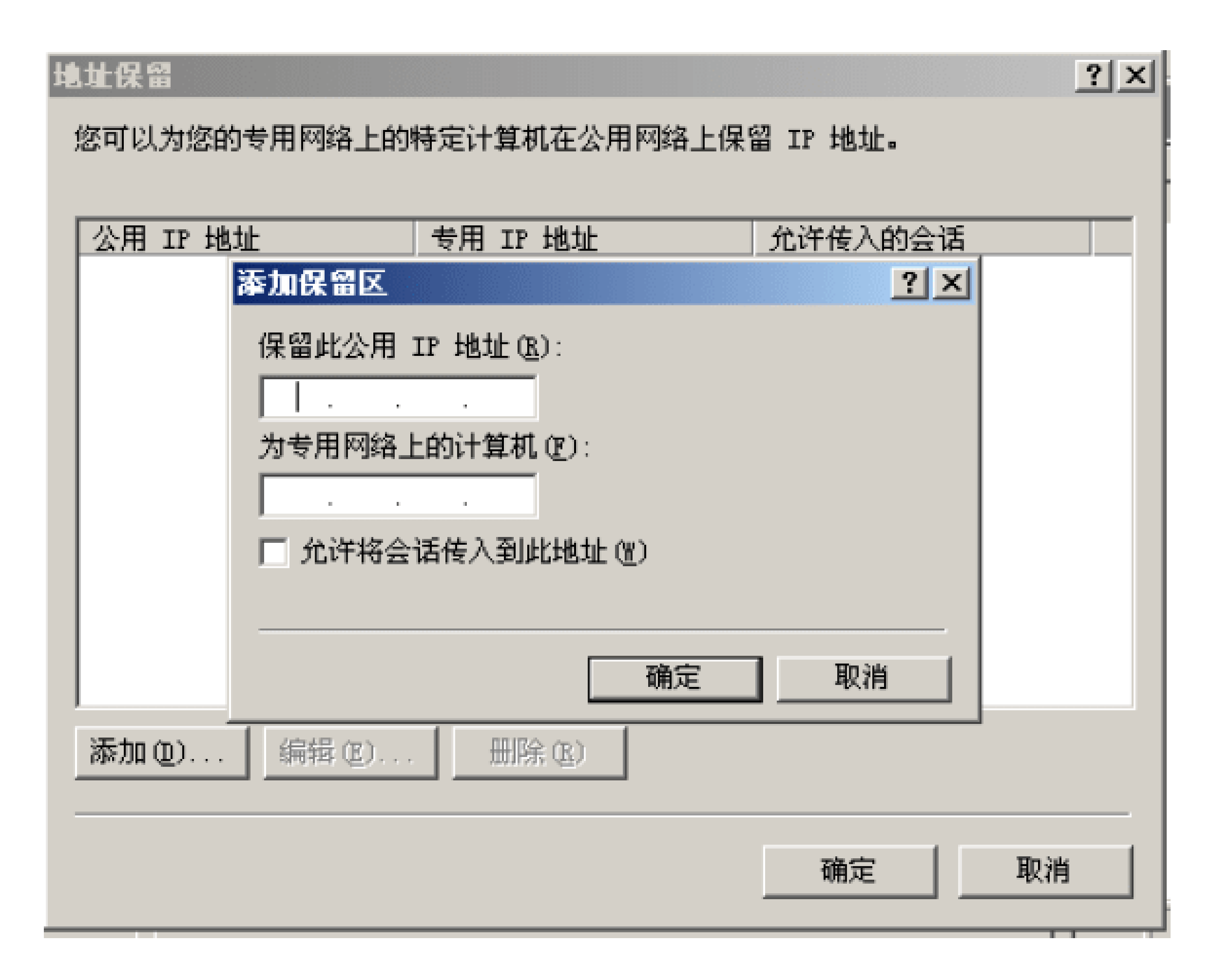


图 3-13 【地址保留】对话框

【问题 3】(3 分)

为保证 Web 服务器能正常对外提供服务，还需要在图 3-14 所示的【服务和端口】选项卡中选中 (7) 复选框。如果要让来自 Internet 的 ping 消息通过 S1，在图 3-15 中至少要选中 (8) 复选框。

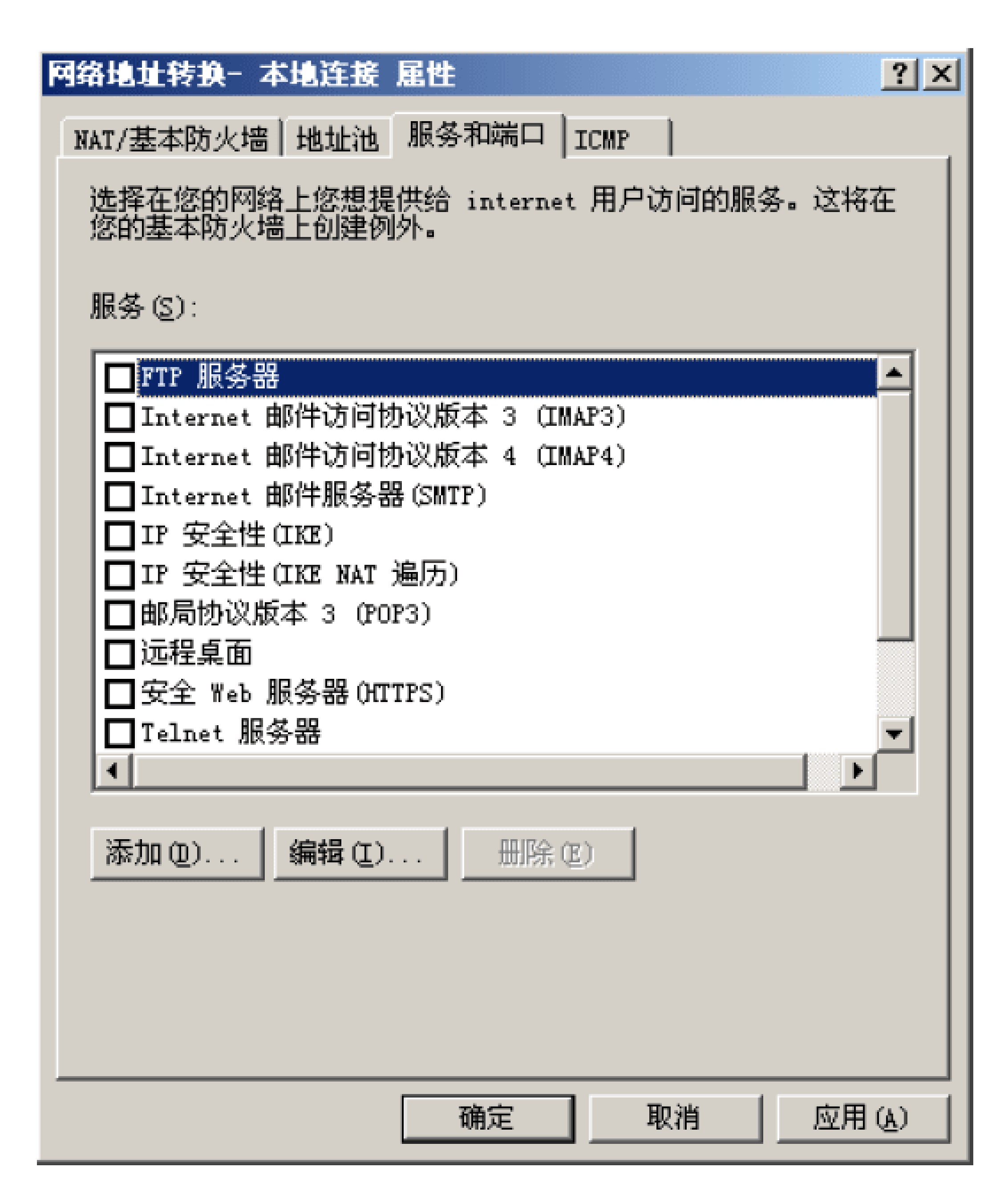


图 3-14 【服务和端口】选项卡

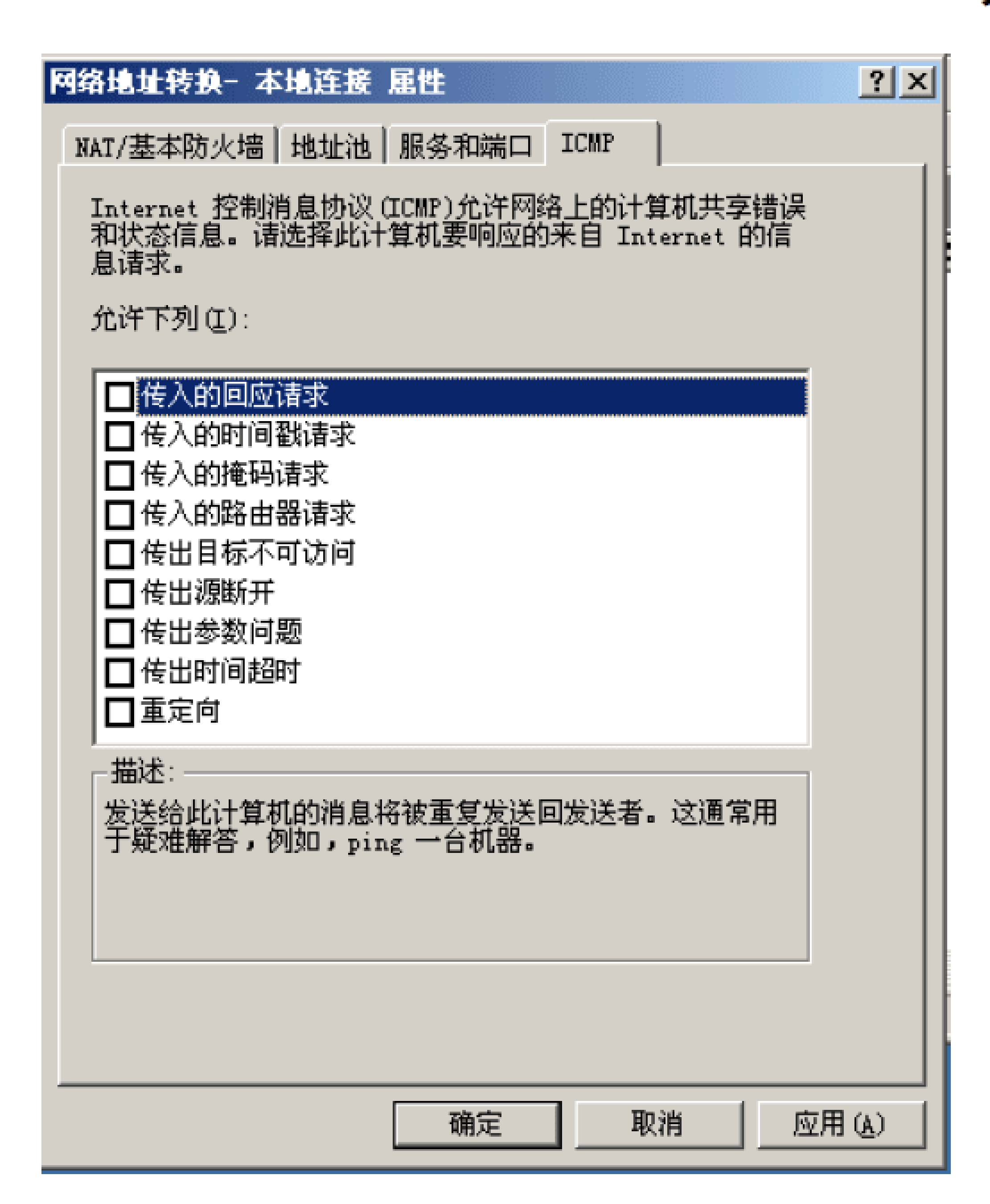


图 3-15　ICMP 选项卡

分析：

【问题 1】

如果接口连接到 Internet，则在【NAT/基本防火墙】选项卡中，选中【公用接口连接到 Internet】单选按钮，并选中【在此接口上启用 NAT】复选框。如果希望用动态数据包筛选器保护公用接口，则选中【在此接口上启用基本防火墙】复选框。故配置 Lan 接口如图 3-11(a)所示，配置 Wan 接口如图 3-11(b)所示。

【问题 2】

由于该公司的公网地址段是 202.134.135.88/29，并且路由器 eth0 的地址为 202.134.135.94。故 Wan 接口的地址范围是 202.134.135.89～202.134.135.93，故(3)题答案为 202.134.135.89，(4)题答案为 202.134.135.93。由于内网中 Web 服务器对外提供的 IP 地址是 202.134.135.92，故(5)答案为 202.134.135.92。(6)题应填入 Web 服务器的地址，即 192.168.1.100。

【问题 3】

Web 服务器也称为 WWW(World Wide Web)服务器，主要功能是提供网上信息浏览服务，Web 服务器可以解析(handles)HTTP 协议。为保证 Web 服务器能正常地对外提供服务，必须有 Web 服务器。如果没有启用 Internet 控制消息协议 (ICMP)允许传入的回应请求，那么传入请求将失败，并生成传入失败的日志项。

答案：

【问题 1】

(1)　如图 3-11(a)所示

(2)　如图 3-11(b)所示

【问题2】

(3) 202.134.135.89

(4) 202.134.135.93

(5) 202.134.135.92

(6) 192.168.1.100

【问题3】

(7) 安全 Web 服务器(HTTPS)

(8) 传入的回应请求

例2 阅读以下说明，回答问题1～问题6，将解答填入答题纸对应的解答栏内。(2009年5月下午试题四)

【说明】

某企业的网络拓扑结构如图3-16所示。

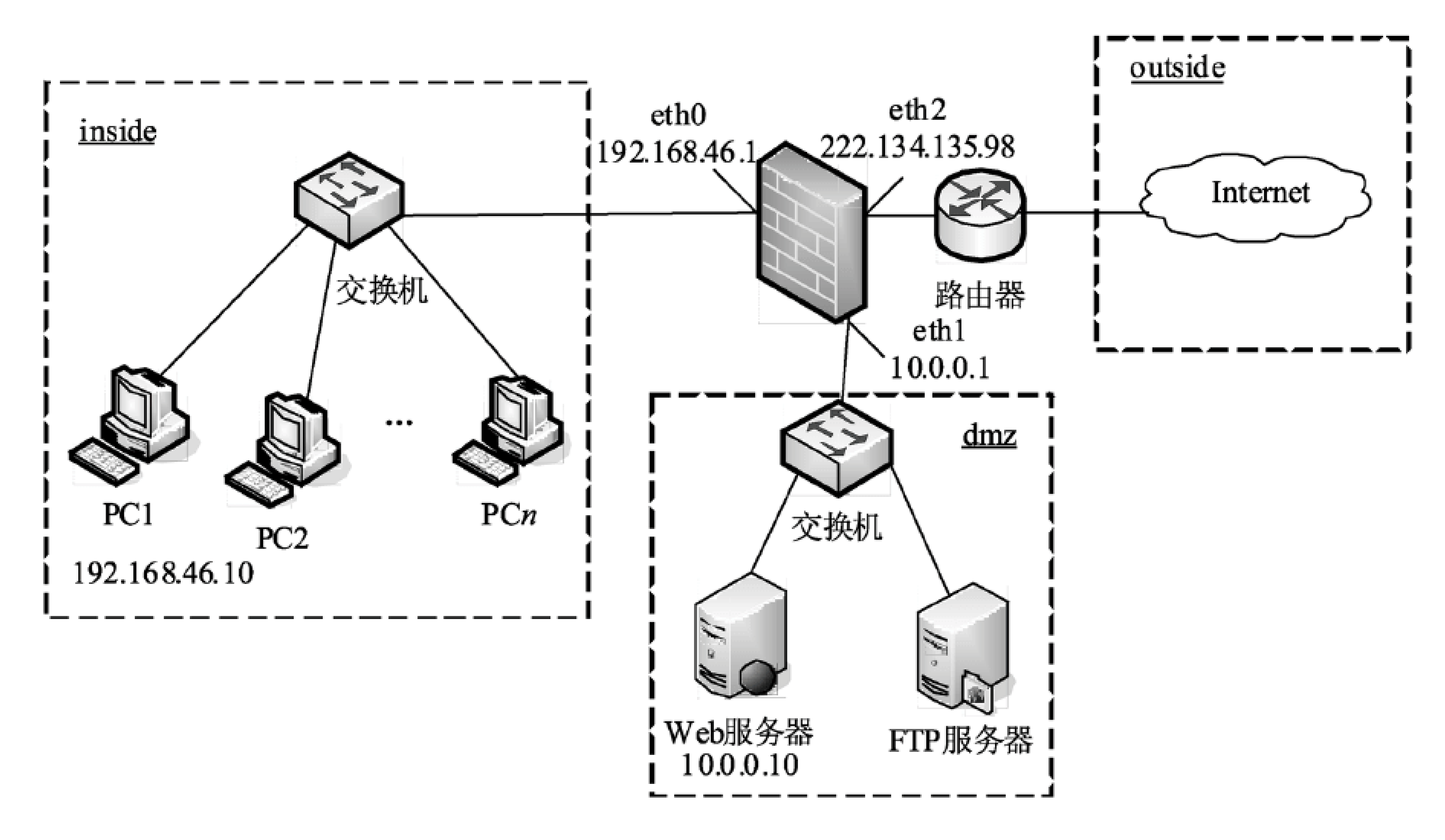


图3-16 某公司网络拓扑结构

【问题1】(2分)

防火墙使用安全区域的概念来表示与其相连接的网络。图3-16中的inside、outside和dmz区域分别对应于Trust区域、Untrust区域和DMZ，不同区域代表了不同的可信度，默认的可信度由高到低的顺序为__(1)__。

A. inside、outside、dmz　　B. inside、dmz、outside

C. outside、dmz、inside　　D. outside、inside、dmz

【问题2】(2分)

包过滤防火墙利用数据包的源地址、目的地址、__(2)__、__(3)__和所承载的上层协议，把防火墙的数据包与设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

【问题3】(4分)

为了过滤数据包，需要配置访问控制列表(ACL)，规定什么样的数据包可以通过？什么样的数据包不能通过？ACL规则由多条permit或deny语句组成，语句的匹配顺序是从上

到下。

语句 access-list 1 deny any any 的含义是__(4)__，该语句一般位于 ACL 规则的最后。

语句 access-list 100 permit tcp anyhost 222.134.135.99 eq ftp 的含义是__(5)__。

【问题 4】(3 分)

请按照图 3-16 所示，完成防火墙各个网络接口的初始化配置。

```
firewall(config)# ip address inside  (6)  255.255.255.0       //配置网口 eth0
firewall(config)# ip address outside  (7)  255.255.255.250   //配置网口 eth2
firewall(config)# ip address  (8)  10.0.0.1 255.255.255.0    //配置网口 eth1
```

【问题 5】(2 分)

如图 3-16 所示，要求在防火墙上通过 ACL 配置，允许在 inside 区域除工作站 PC1 外的所有主机都能访问 Internet，请补充完成 ACL 规则 200。

```
access-list 200  (8)  host 192.168.46.10 any
access-list 200  (10)  192.198.46.0 0.0.0.255 any
```

【问题 6】(2 分)

如图 3-16 所示，要求在防火墙上配置 ACL，允许所有 Internet 主机访问 DMZ 中的 Web 服务器，请补充完成 ACL 规则 300。

```
access-list 300 permit tcp  (11)  host 10.0.0.10 eq  (12) 。
```

分析：

【问题 1】inside 区域(内网)是指位于防火墙之内的可信网络，是防火墙要保护的目标。

dmz 区域(非军事化区)是一个隔离的网络，可以位于防火墙之外，也可位于防火墙之内，安全敏感度和保护强度较低，一般用开放式方法提供公共网络服务的设备。对于外部用户，dmz 区域通常是可以访问的，这样就允许外部用户访问企业的公开信息，但不允许他们访问企业的内部网络。

而 outside 区域(外网)是指处于防火墙之外的公共开放网络，是不被信任的区域。

【问题 2】包过滤防火墙在网络的入口对通过的数据包进行检查，每个 IP 包的字段都会被检查，包括源地址、目的地址、源端口号、目的端口号、协议等，然后将这些信息与设立的过滤规则相比较，与规则不匹配的包就会被丢弃，否则按规则来处理。

【问题 3】使用 access-list 命令配置访问控制列表 ACL 的格式为：

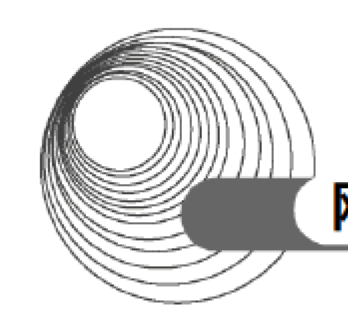
```
access-list access-list-number {permit | deny } protocol source wildcard-mask
destination wildcard-mask [operator] [operand]
```

其中，permit 表示允许数据包通过；而 deny 则表示拒绝数据包通过。wildcard-mask 为通配符掩码，是子网掩码的反码；operator 表示操作，包括：lt(小于)、gt(大于)、eq(等于)、neq(不等于)；operand 表示操作数，指的是端口值。

语句 access-list 1 deny any any 将禁止所有 IP 数据包通过防火墙。

语句 access-list 100 permit tcp anyhost 222.134.135.99 eq ftp 会允许所有主机访问 222.134.135.99 的 FTP 服务。

【问题 4】防火墙使用 ip address 命令配置网卡的 IP 地址。其命令格式为：




```
ip address {outside | inside | dmz } ip-address mask
```

网口 eth0 连接内网、网口 eth1 连接 dmz 区域、网口 eth2 连接外网。防火墙在内网的 IP 地址是 192.168.46.1，在 dmz 区域的 IP 地址是 10.0.0.1，在外网的 IP 地址是 222.134.135.98。因此，配置相应网口的命令如下。

配置网口 eth0 的命令为：ip address inside 192.168.46.1 255.255.255.0。

配置网口 eth1 的命令为：ip address dmz 10.0.0.1 255.255.255.0。

配置网口 eth2 的命令为：ip address outside 222.134.135.98 255.255.255.252。

【问题 5】要允许在 inside 区域除工作站 PC1 外的所有主机都能访问 Internet，则首先应配置拒绝工作站 PC1 访问 Internet 的控制语句，为：access-list 200 deny host 192.168.46.10 any。然后再配置允许内网其他所有主机访问 Internet 的控制语句，内网的网络地址为 192.198.46.0，子网掩码为 255.255.255.0，通配符掩码为 0.0.0.255，因此配置语句为：access-list 200 permit 192.198.46.0 0.0.0.255 any。

【问题 6】dmz 中的 Web 服务器的 IP 地址为 10.0.0.10，端口为 80，允许所有 Internet 主机访问 dmz 中的 Web 服务器，则配置语句为：access-list 300 permit tcp any host 10.0.0.10 eq 80。

答案：

【问题 1】(1) B

【问题 2】(2) 源端口号　(3) 目的端口号

【问题 3】(4) 过滤所有数据包(或禁止所有 IP 数据包通过防火墙)

(5) 允许所有主机访问 222.134.135.99 的 FTP 服务。

【问题 4】(6) 192.168.46.1 (7) 222.134.135.98　(8) DMZ

【问题 5】(9) deny　(10) permit

【问题 6】(11) any　(12) www(或 80)

例 3　阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2007 年 11 月下午试题四)

【说明】

图 3-17 是某企业网络拓扑结构。

其中，图中各项说明如下。

- Router 是屏蔽路由器。
- FireWall 是防火墙，通过其上的默认 Web 服务端口能够实现对防火墙的配置。
- Console 是管理员控制台。
- MailSrv 是邮件服务器。
- FTPSrv 是 FTP 服务器。
- 区域 IV 是企业日常办公网络，定义为 LocalNet。

【问题 1】(4 分)

该网络中，__(1)__是 DMZ。为使该企业网能够接入 Internet，路由器的接口①能够使用的 IP 地址是__(2)__。

(1) A. 区域 I　B. 区域 II　C. 区域 III　D. 区域 IV

(2)　A. 10.1.1.1　　　　　B. 100.1.1.1
　　 C. 172.30.1.1　　　　D. 192.168.1.1

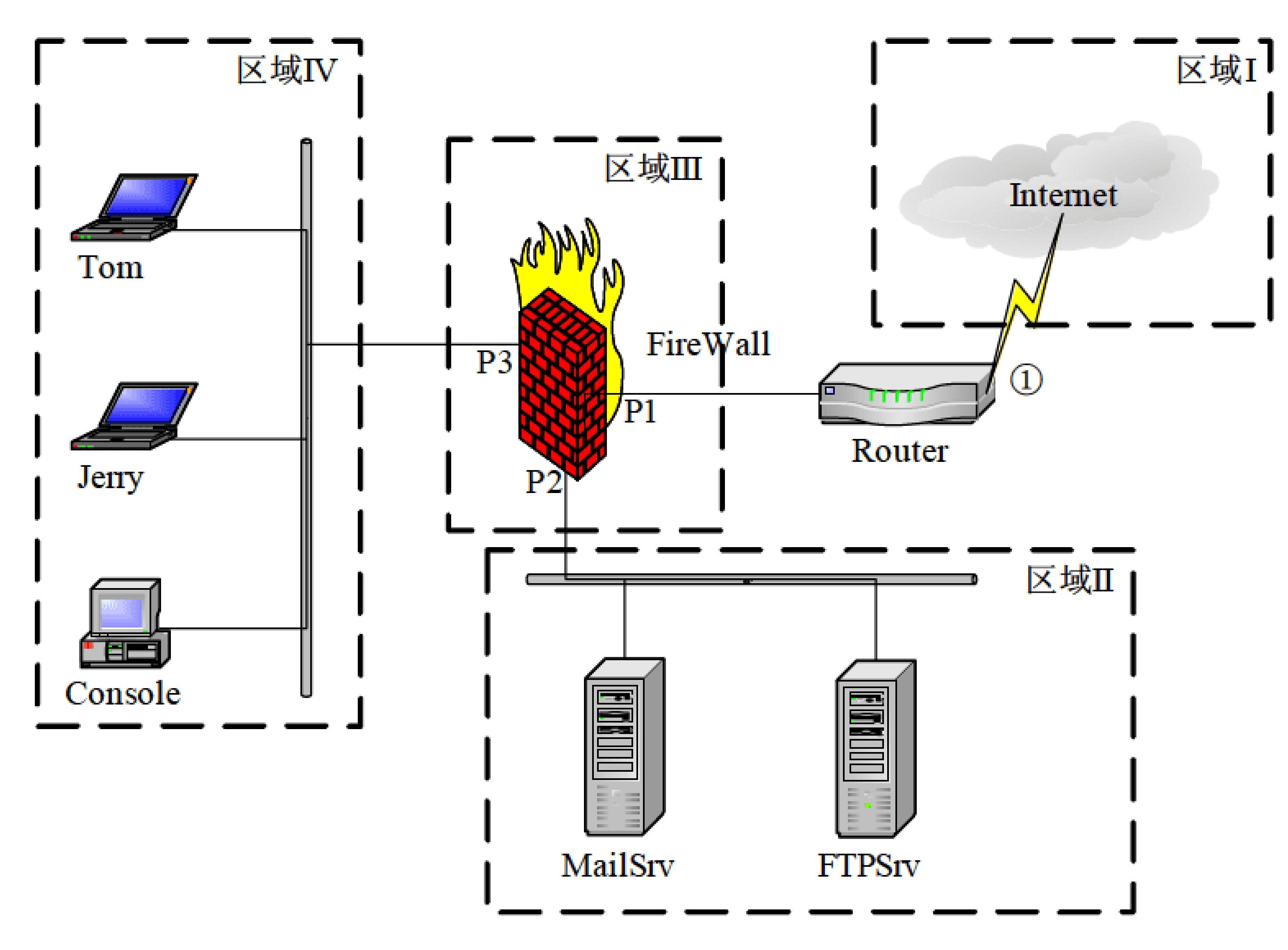


图 3-17　某企业网络拓扑结构

【问题 2】(3 分)

对于区域 IV 而言，进入区域 IV 的方向为“向内”，流出区域 IV 的方向为“向外”。表 3-1 中防火墙规则表示：防火墙允许 Console 与任何区域 IV 以外的机器收发 POP3 协议数据包，并在此基础上拒绝所有其他通信。

表 3-1　防火墙访问规则列表(1)

源	目　的	方　向	协　议	行　动
Console	Any	向外	POP3	允许
Any	Console	向内	POP3	允许
Any	Any	Any	Any	拒绝

若允许控制台 Console 仅通过防火墙开放的 Web 服务配置防火墙 FireWall，则在防火墙中应增加表 3-2 中的策略。

表 3-2　防火墙访问规则列表(2)

源	目　的	方　向	协　议	行　动
Console	FireWall	(3)	(4)	允许
FireWall	Console	向内	(4)	(5)

(4)　A. TCP　　　B. UDP　　　C. HTTP　　　D. SNMP

【问题 3】(3 分)

如果 FireWall 中有表 3-3 中的过滤规则，则__(6)__。

表 3-3　防火墙访问规则列表(3)

源	目　的	方　向	协　议	行　动
LocalNet	FTPSrv	P3→P2	FTP	允许
FTPSrv	LocalNet	P2→P3	FTP	允许
Not(LocalNet)	FTPSrv	P1→P2	FTP	拒绝

A. 区域 IV 能访问 FTPSrv 进行文件上传与下载，Internet 只能上传不能下载
B. 区域 IV 能访问 FTPSrv 进行文件上传与下载，Internet 只能下载不能上传
C. 区域 IV 和 Internet 都能访问 FTPSrv 进行文件上传与下载
D. 只有区域 IV 能访问 FTPSrv 进行文件上传与下载

【问题 4】(5 分)

要求管理员在网络中的任何位置都能通过在 MailSrv 上开放的默认 Telnet 端口登录 MailSrv，实现对 MailSrv 的配置。因此，需要在防火墙中添加如表 3-4 所示的规则(*代表 P1、P2、P3 中的任意一个或几个)。

表 3-4　防火墙访问规则列表(4)

源	目　的	方　向	协　议	源 端 口	目的端口	ACK	行　动
Any	MailSrv	*→P2	(7)	(8)	(9)	(10)	允许
MailSrv	Any	P2→*	(7)	(9)	(8)	(11)	允许

(7) A. TCP　B. UDP　C. TLS　D. ICMP
(8) A. <1023　B. >1023　C. <1024　D. >1024
(9) A. 21　B. 23　C. 25　D. 27
(10) A. 0　B. 1　C. 0 或 1
(11) A. 0　B. 1　C. 0 或 1

分析：

【问题 1】考查非军事区的概念以及私有/公网 IP 的基础知识。

【问题 2】考查常见网络应用层协议的基础知识。控制台 Console 仅通过防火墙开放的 Web 服务配置防火墙 FireWall，实际上需要设置防火墙，允许开放两者之间的 HTTP 协议通信。

【问题 3】考查 FTP 协议的基础知识。题目中虽然只是配置防火墙限制单向通信，但对于 FTP 协议来说，则限制了参与通信的两个实体之间进行交互。因此，只有区域 IV 能访问 FTPSrv 进行文件的上传与下载。

【问题 4】主要考查 TCP 协议的基础知识。Telent 需要使用 TCP 协议的端口 23。系统中 TCP 端口号小于等于 1023 的端口被保留使用，系统自动分配的端口号会大于 1023。发起建立 TCP 连接，以及对这一命令进行响应时，还需要对 ACK 标志位进行相应操作。

答案：

【问题 1】

(1)　B　　　　(2)　B

【问题 2】

(3)　向外　　　　(4)　C　　　　(5)　允许

【问题 3】

(6)　D

【问题 4】

(7)　A　　　　(8)　B　　　　(9)　B

(10) C　　　　(11) B

例 4　阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2007 年 5 月下午试题四)

【说明】

某企业的网络安装防火墙后，其拓扑结构如图 3-18 所示。

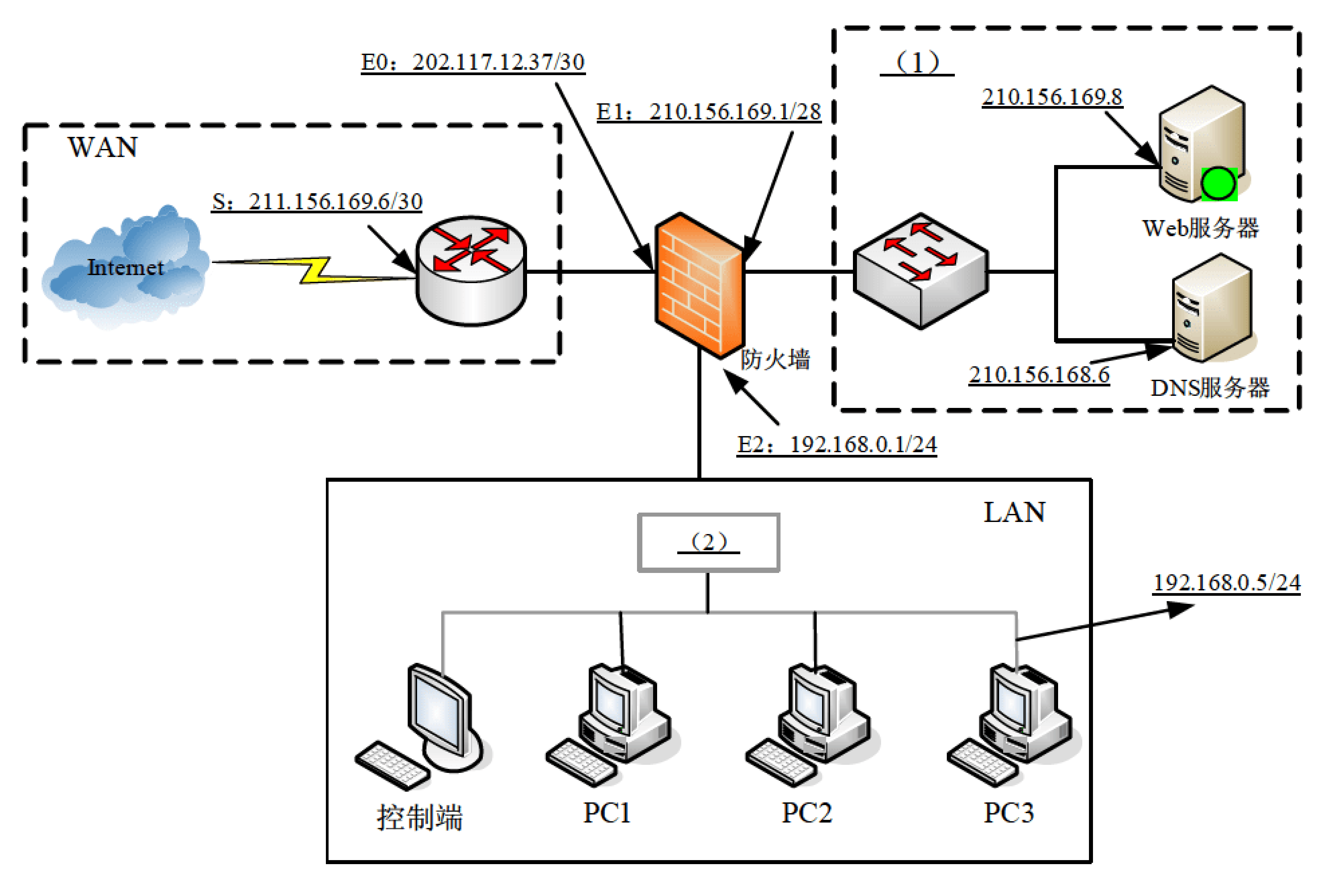


图 3-18　某企业网络拓扑结构

【问题 1】(3 分)

为图 3-18 中的 (1) 处选择合适的名称。

A. 服务区　　　　B. DMZ　　　　C. 堡垒区　　　　D. 安全区

【问题 2】(3 分)

为图 3-18 中的 (2) 处选择合适的设备。

A. 远程访问服务器　　　　B. 以太网交换机

C. 调制解调器

【问题3】(3分)

以下哪一项属于配置该防火墙的目的？ (3) 。

A. 防止未授权的通信进出内部网络

B. 进行域名解析

C. 对IP包进行协议转换

D. 对进出内部网络的数据包进行加密

【问题4】(4分)

参照图3-18所示的界面，添加以下访问控制规则，以禁止PC3访问地址为210.156.169.8的Web服务器。

序　号	描　述	生　效	策　略	源地址	目的地址	目的端口	协　议
3	WWW访问控制	是	(4)	(5)	(6)	80	(7)

(4) A. 允许　B. 禁止

(5) A. 192.168.0.1　B. 192.168.0.5　C. 210.156.169.6　D. 210.156.169.8

(6) A. 192.168.0.1　B. 192.168.0.5　C. 210.156.169.6　D. 210.156.169.8

(7) A. TCP　B. UDP

【问题5】(2分)

参照图3-18所示的界面，添加以下配置记录，使得Lan中的主机访问Internet Web服务时，能够隐藏内部主机的源地址。

源 地 址	源 端 口	目的地址	目的端口	协　议	转换后的源地址	转换后的源端口
内网网段	ANY	(8)	80	TCP	(9)	不变

(8) A. 192.168.0.5　B. 210.156.169.6　C. 202.117.12.37　D. ANY

(9) A. 192.168.0.5　B. 210.156.169.6　C. 202.117.12.37　D. ANY

分析：

【问题1】本题考查的是防火墙的类型和基本结构。

在防火墙的设计和实施中，目前使用最多的是屏蔽子网类防火墙。屏蔽子网系统是在内部网络与外部网络之间建立一个被隔离的子网，也称为非军事区(dmz)，用两台分组过滤路由器将这一子网分别与内部和外部网络分开。该系统进一步实现内部主机的安全性，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信。因此，WWW和FTP等服务器一般放置于dmz中。

【问题2】本题考查的是防火墙中内部网络的连接方式和设备。

在屏蔽子网防火墙系统中需要配置三个网络：Internet、dmz和受保护网络。由于Internet很难与内部网络进行通信，因此防火墙管理员不需要指定内部网络到Internet之间的路由。内部网络如果是一个小型局域网，那么可以使用局域网交换机连接多台PC。

【问题3】本题考查的是防火墙的功能。

一般来说，防火墙通常有以下几大功能。

- 防止非法用户进入内部网络。

- 利用 NAT 功能将私网地址转换为公网地址，提高内部网络的安全性。
- 实施安全策略的确认和授权。
- 方便对网络的安全性进行监控，产生日志和报警。
- 防火墙可以对进出网络的所有通信进行审计和记录。
- 可以对网络设备的访问权限进行监督。

【问题 4】本题考查的是防火墙访问控制规则的配置。

通过配置访问控制策略可以使得防火墙能够对进出网络的通信进行控制，过滤规则一般放置在连接内部和外部网络的路由器上。

【问题 5】本题考查的是防火墙的地址隐藏功能配置。

NAT 是防火墙的一大功能，通过这个功能可以对内部网络地址进行隐蔽，从而防止对网络地址的跟踪。

答案：

【问题 1】

(1)　B

【问题 2】

(2)　B

【问题 3】

(3)　A

【问题 4】

(4)　B　　(5)　B　　(6)　D　　(7)　A

【问题 5】

(8)　D　　(9)　C

例 5　阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2008 年 11 月下午试题四)

【说明】

IE 浏览器支持 HTTP、HTTPS、FIT 等多种协议。

【问题 1】(每空 1 分，共 2 分)

如果在 IE 地址栏中输入 192.168.0.1，如图 3-19 所示，则默认的通信协议是__(1)__；如果要访问 FIT 服务器(地址为 192.168.0.2)，应该在地址栏中输入__(2)__。

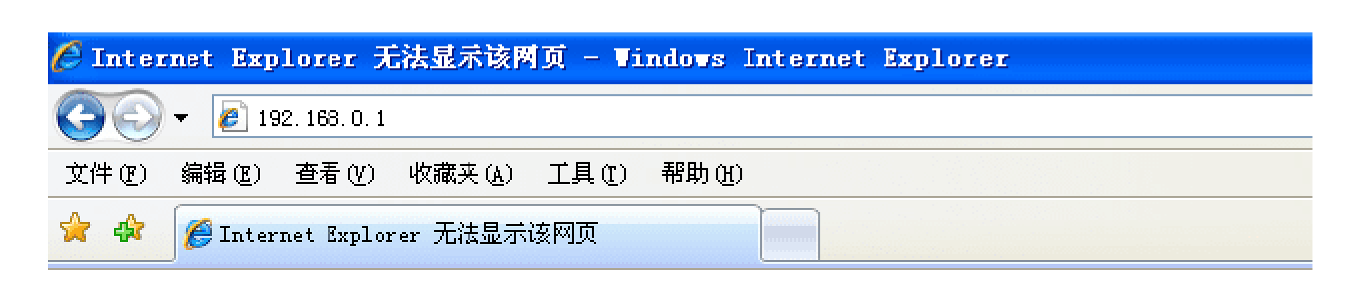


图 3-19　IE 浏览器界面

【问题 2】(空(3)、(4)各 2 分，空(5)、(6)各 1 分，共 6 分)

IE 浏览器的安全区设置可以对被访问的网站设置信任度，IE 浏览器包含了四个安全区域：Internet、本地 Internet、可信站点和受限站点，如图 3-20 所示，其中受限站点默认的安全级别为__(3)__。



图 3-20 【Internet 选项】对话框

对于公网上某个有害站点，可以通过将该站点加入到__(4)__的方法来禁止访问；对于公网上某个确认安全的站点，可以通过将该站点加入到__(5)__或__(6)__的方法来确保对该站点的正常访问，同时不降低安全性。

【问题 3】(每空 1 分，共 3 分)

IE 浏览器提供的“自动完成表单和 Web 地址”功能方便了操作，同时可能造成用户名和密码被泄露，因此在输入用户名和密码之前就应该关闭该功能，方法是在如图 3-21 所示的复选框中取消选中__(7)__选项，如果在此操作之前已经输入了用户名和密码，则应该通过执行图 3-22 中的__(8)__和__(9)__选项来避免用户名和密码泄露。

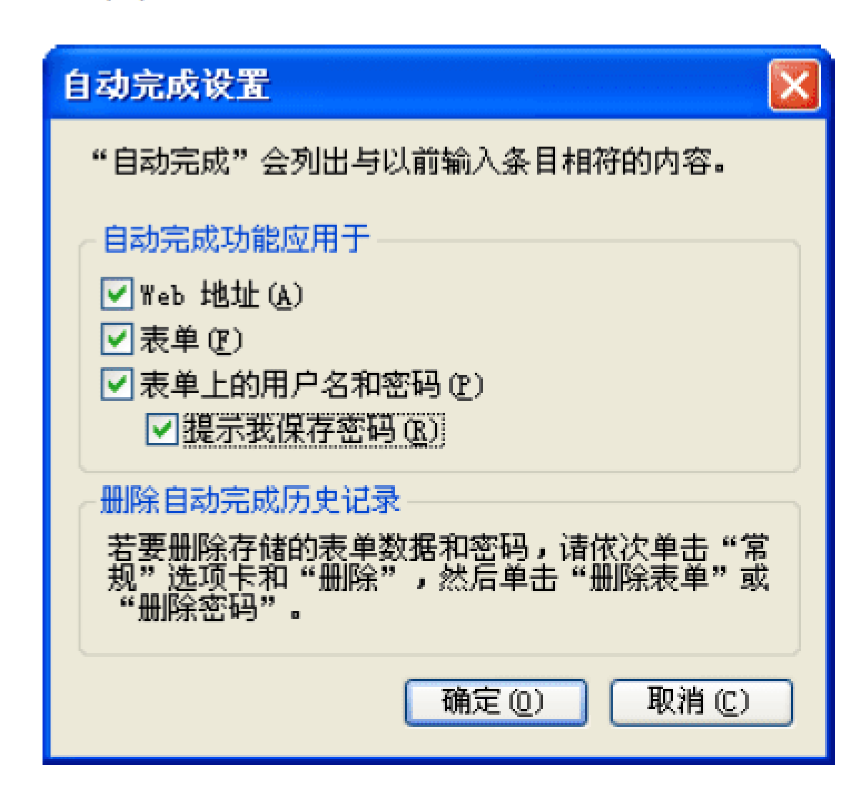


图 3-21 【自动完成设置】对话框

【问题 4】(每空 2 分，共 4 分)

IE 浏览器支持用于 Internet 内容分级的 PICS(Platform for Internet Content Selection)标准。通过设置分级审查功能，可帮助用户控制计算机访问的 Internet 信息的类型(见图 3-23)。例如要限定 IE 只能访问 www.abc.com 网站，设置步骤如下。

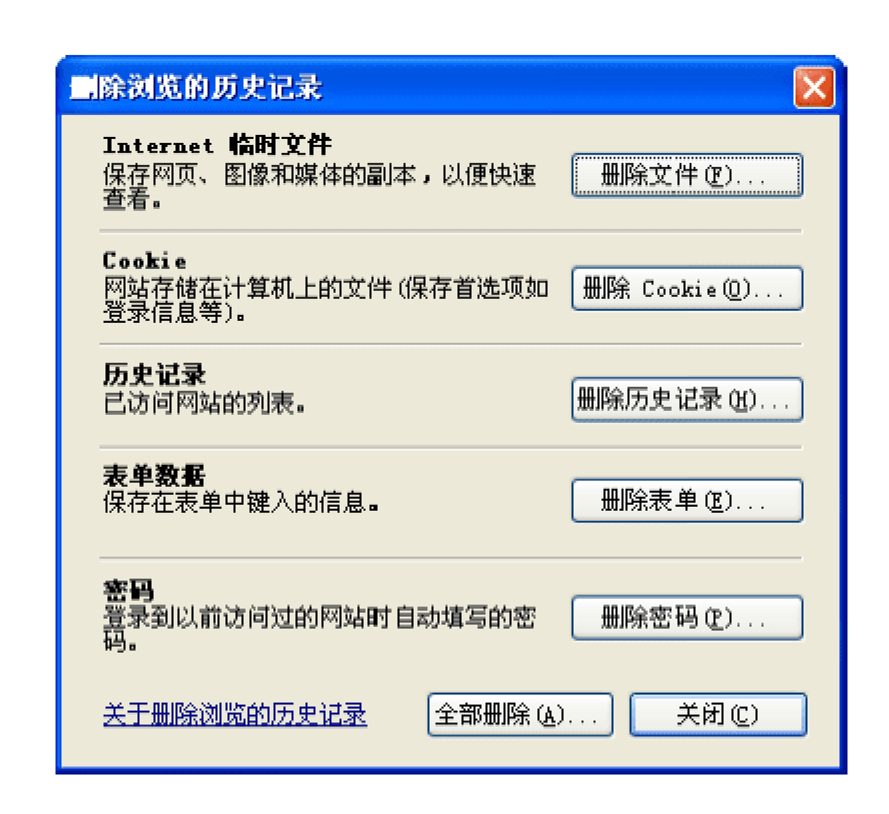


图 3-22　【删除浏览的历史记录】对话框

① 在 IE 浏览器的__(10)__菜单中打开【Internet 选项】对话框。

② 切换至【内容】选项卡，在分级审查区域中单击【启用】按钮。

③ 在弹出的【内容审查程序】对话框中，将【分级】选项卡中的滑块调到 0。

④ 切换到【许可站点】选项卡，在【允许该站点】文本框中填入__(11)__，单击【始终】按钮后单击【确定】按钮创建监护人密码。

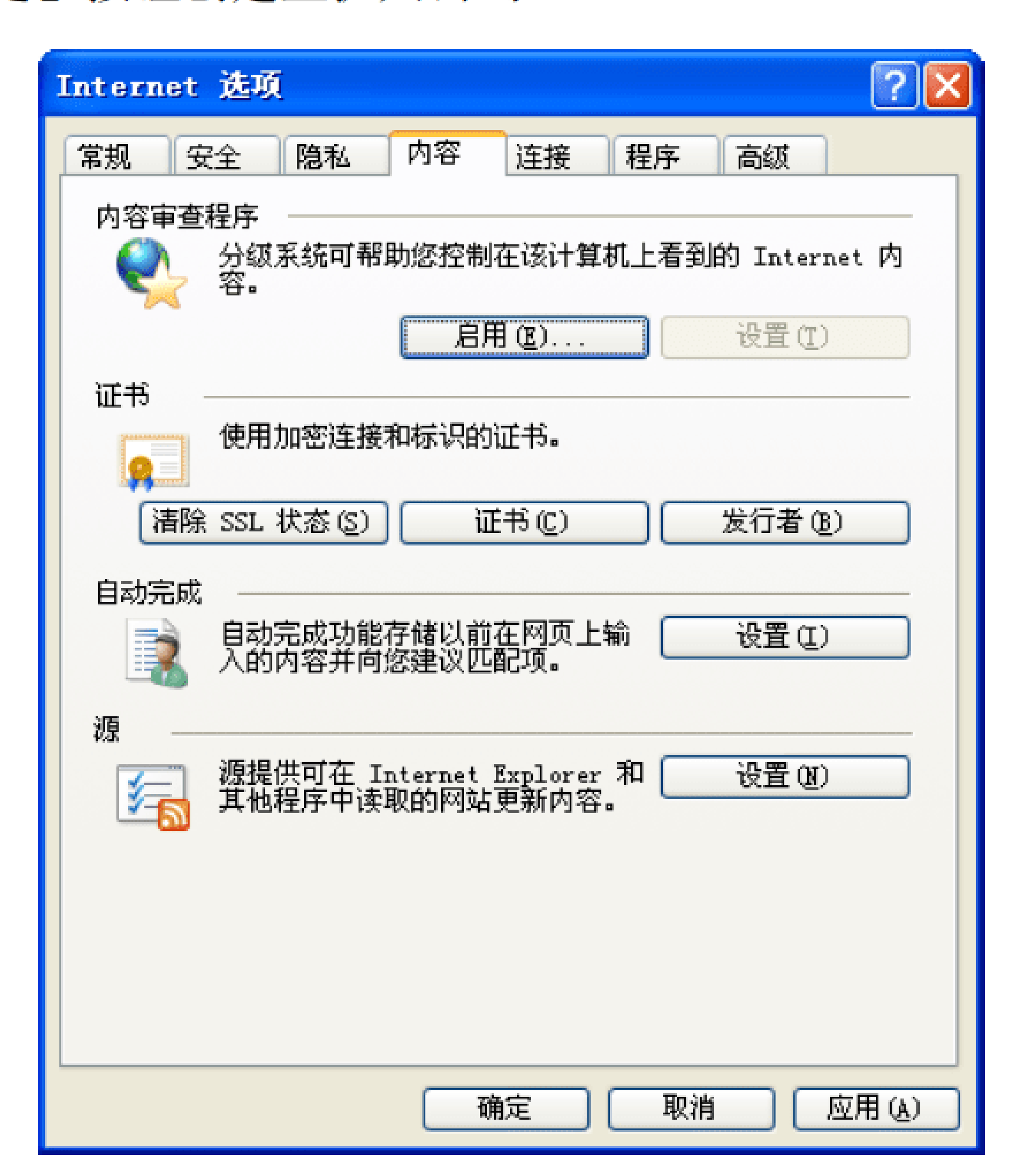


图 3-23　【内容】选项卡

分析：

【问题 1】IE 浏览器支持 HTTP、FTP、Telnet、Gopher 等多种协议，其中默认支持的是 HTTP 协议。如果在 IE 地址栏中直接输入 IP 地址，则 IE 浏览器会采用 HTTP 协议与该 IP 地址所属的 Web 服务器通信。如果要用其他协议通信，则在地址栏中必须指明协议类型，当要访问 IP 地址为 192.168.0.2 的 FTP 服务器时，应该在地址栏中输入 ftp://192.168.0.2。

【问题 2】IE 浏览器包含了四个安全区域：Internet、本地 Intranet、可信站点和受限站

点。Internet 区域的默认安全级别为“中”，本地 Intranet 区域的默认安全级别为“中低”，可信站点区域的默认安全级别为“低”，受限站点区域的默认安全级别为“高”。可见受限站点的安全级别为高。

受限站点区域适用于包含可能损坏计算机或文件的网站，对于有害站点可分配到该区域，以禁止或限制对该网站的访问。Internet 区域包含了所有未放在其他区域的 Web 站点，可信站点区域包含信任的站点，相信这些站点不会损坏计算机或文件。可以将公网上某个确认安全的站点加入 Internet 区域或可信站点区域，以降低对该站点的安全限制，从而确保对该站点的正常访问。

【问题 3】自动完成功能是指在网页上填写一些表单时，让 IE 浏览器自动记下所填写的内容，下次填写同样的表单时可以自动调出以前的内容，但这也带来了安全隐患。为了避免用户名和密码泄露，可在【自动完成设置】对话框中取消对【表单上的用户名和密码】复选框的选中，以禁止对用户名和密码使用自动完成功能。如果在此操作之前已经输入了用户名和密码，则应该在【删除浏览的历史记录】对话框中执行删除表单和删除密码操作，以删除保存过的表单内容和登录网站时填写的密码。

【问题 4】在 IE 中设置分级审查功能，可对 IE 进行信息限制，屏蔽掉一些不想让上网用户浏览的站点。限定 IE 只能访问 www.abc.com 网站的设置步骤如下。

① 在 IE 浏览器的【工具】菜单中选择【Internet 选型】命令，打开【Internet 选项】对话框。

② 切换至【内容】选项卡，在【内容审查程序】区域中单击【启用】按钮。

③ 在弹出的【内容审查程序】对话框中，将【分级】选项卡中的滑块调到 0。

④ 切换到【许可站点】选项卡，在【允许该站点】文本框中填入 www.abc.com，单击【始终】按钮后单击【确定】按钮，创建监护人密码。

答案：

【问题 1】

(1) HTTP　(2) ftp://192.168.0.2

【问题 2】

(3) 高　(4) 受限站点　(5) 本地 Internet　(6) 可信站点

注：(5)和(6)的答案可以互换。

【问题 3】

(7) 表单上的用户名和密码　(8) 删除表单　(9) 删除密码

注：(8)和(9)的答案可以互换。

【问题 4】

(10) 工具　(11) www.abc.com

例 6　阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2008 年 5 月下午试题四)

【说明】

某公司在 Windows 2003 中安装 IIS 6.0 作为 Web 服务器，IP 地址为 211.120.114.3，端口号为 8080，并在 IIS 中配置 HTTPS 实现安全的 Web 通信，如图 3-24 所示。

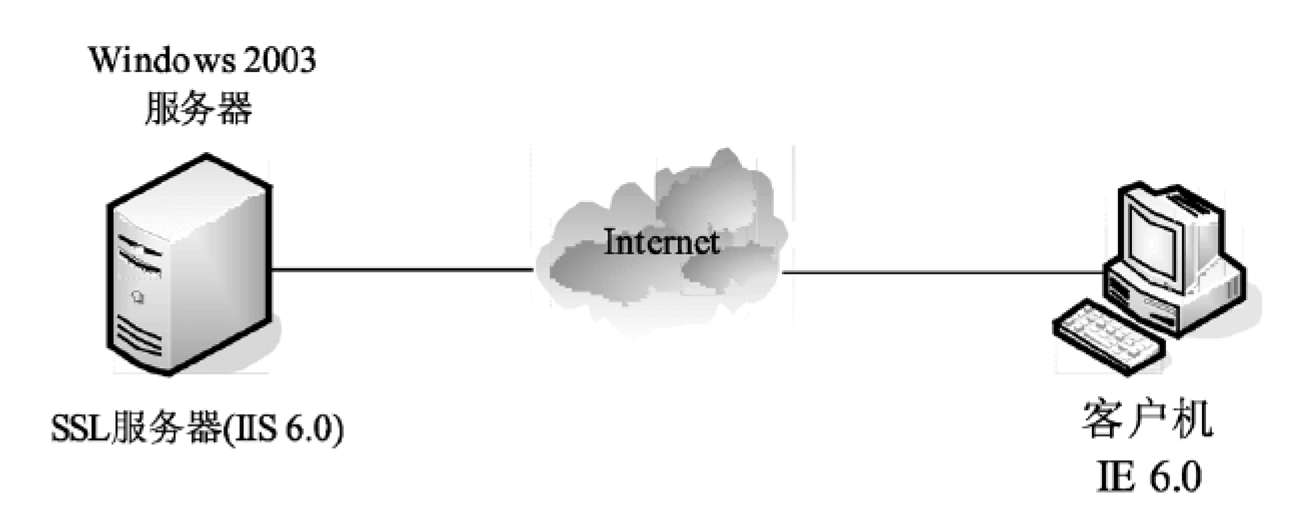


图 3-24　安全的 Web 通信示意

【问题 1】(4 分)

IIS 6.0 安装的硬盘分区最好选用 NTFS 格式，是因为 (1) 和 (2) 。

A. 可以防止网页中的 Applet 程序访问硬件中的文件

B. 可以针对某个文件或文件夹给不同的用户分配不同的权限

C. 可以使用系统自带的文件加密系统对文件或文件夹进行加密

D. 可以在硬盘分区中建立虚拟目录

【问题 2】(2 分)

HTTPS 工作在 (3) 层，为浏览器和 Web 服务器提供安全信息交换，它运行在安全 (4) 之上。

(3) A. 网络层　　B. 传输层　　C. 应用层　　D. 会话层

(4) A. 网关　　B. 套接口　　C. 密钥　　D. 物理连接

【问题 3】(4 分)

在配置 IIS 6.0 时，需首先向 (5) 申请并安装数字证书，然后 Web 服务器才能支持 SSL 会话。

在 IIS 中安装 SSL 分 5 个步骤， (6) →提交数字证书申请→ (7) →在 IIS 服务器上导入并安装证书→ (8) 。

A. 下载证书文件

B. 生成证书请求文件

C. 配置身份验证方式和 SSL 安全通道

【问题 4】(3 分)

如果希望 Web 服务器只接受 HTTPS 请求，而不接受未加密的 HTTP 请求，加密密钥为 128 位，并且无需为客户端提供数字证书，在图 3-25 中该如何配置？

【问题 5】(2 分)

如果用户需要通过 SSL 安全通道访问该 Web 网站，可在 IE 地址栏中输入 (8) 。

分析：

【问题 1】

NTFS 文件系统有很好的安全性和稳定性，有以下显著特点。

- NTFS 分区为用户权限作出了非常严格的限制，每个用户都能按照系统赋予的权限进行操作。并且每个文件或文件夹都可以单独地分配一个许可，可以防止未授权用户访问文件或文件夹。

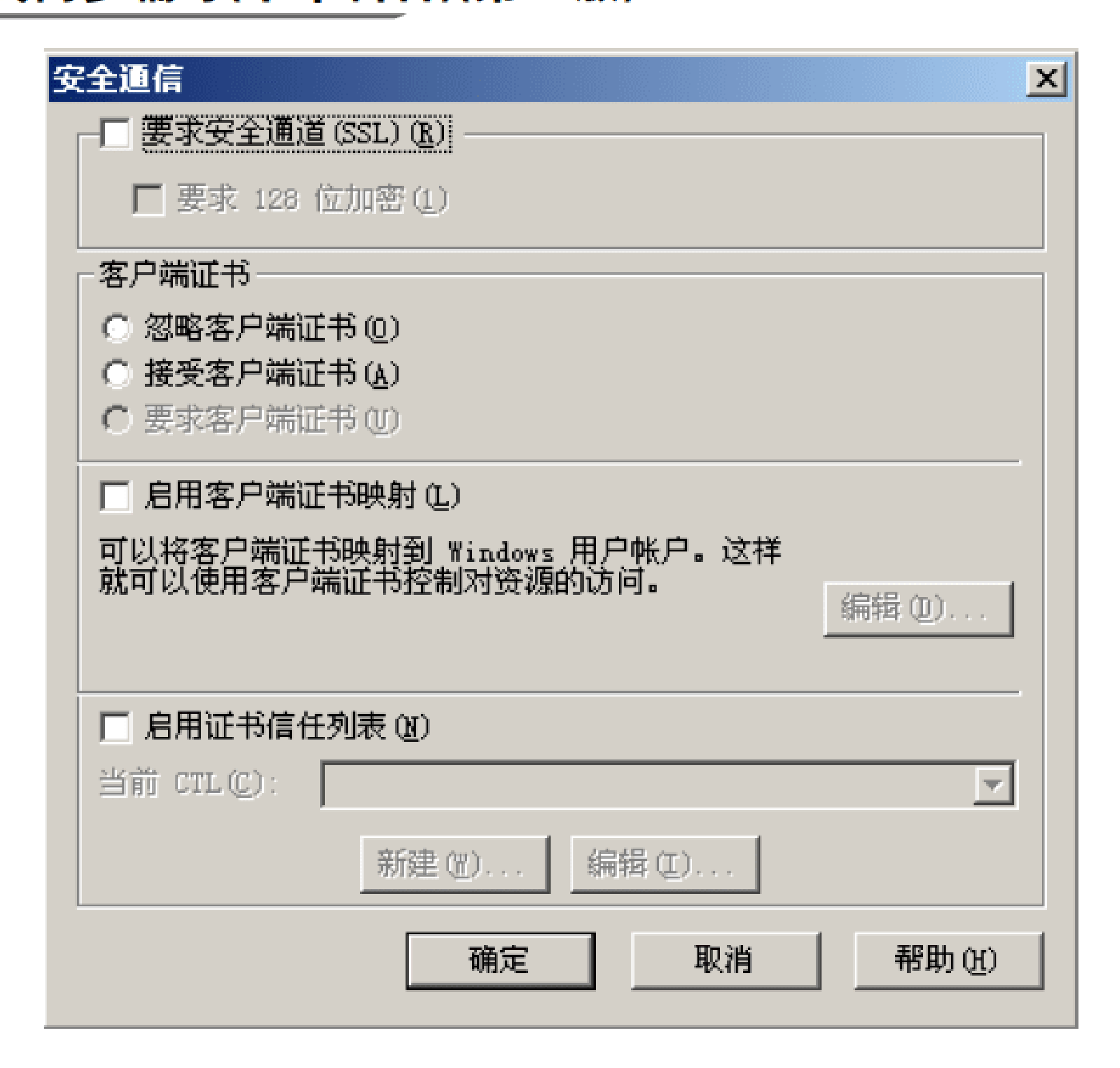


图 3-25 【安全通信】对话框

- NTFS 支持对单个文件的压缩和加密。
- NTFS 可以支持的文件大小可达 64GB，支持更大的分区大小，最小磁盘分区为 100MB，推荐最大分区为 2TB。
- 对于超过 4GB 以上的硬盘，使用 NTFS 分区，可以减少磁盘碎片的数量。
- NTFS 事物日志自动记录所有文件夹或文件更新，当出现系统损坏或电源故障等问题而引起操作失败后，系统能够利用日志文件重做或回复未成功的操作。

【问题 2】安全套接层 SSL 是传输层安全协议，用于实现 Web 安全通信。SSL 在 Web 安全通信中被称为 HTTPS。

【问题 3】要使用 SSL 安全机制，必须为 Windows Server 2003 系统安装数字证书服务，然后申请并安装证书，而数字证书是向 CA 申请的。

安装的步骤如下。

第一步：安装证书服务。

① 在【控制面板】中，打开【添加或删除程序】窗口，单击【添加或删除 Windows 组件】选项，打开【Windows 组件向导】对话框。

② 在【组件】列表框中选中【证书服务】复选框，单击【下一步】按钮。

③ 打开【CA 类型】界面，选择 CA 类型，如选中【独立根 CA】单选按钮，单击【下一步】按钮，如图 3-26 所示。

④ 打开【CA 识别信息】界面，在【此 CA 的公用名称】文本框中为 CA 服务器取个名字，并设置证书的有效期，如图 3-27 所示。

⑤ 打开【证书数据库设置】对话框，指定证书数据库和证书日志的位置，单击【下一步】按钮。

⑥ 系统开始配置组件，完成安装。

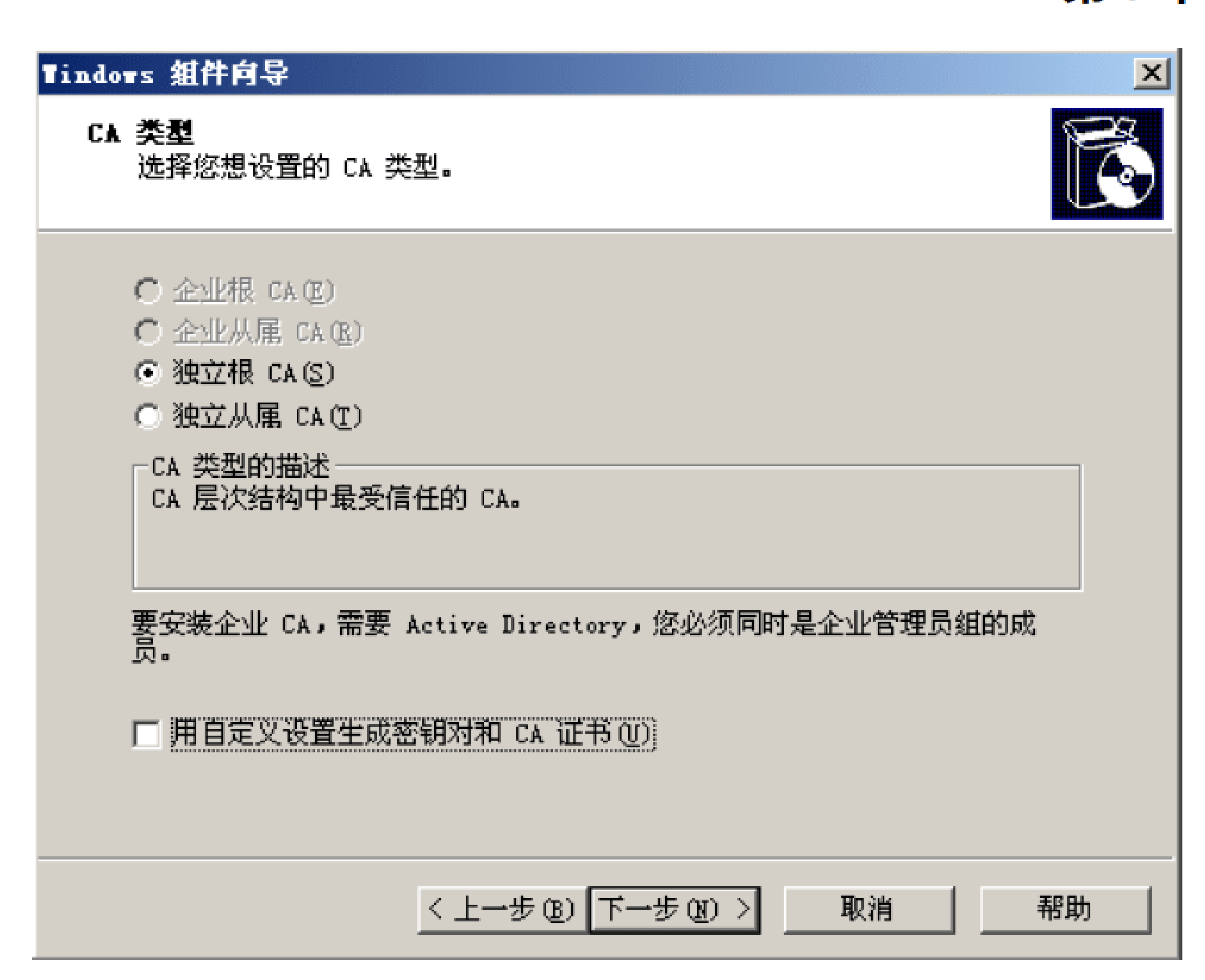


图 3-26　【CA 类型】界面



图 3-27　【CA 识别信息】界面

第二步：生成证书请求文件。安装证书服务之后，就可以创建请求证书文件了。

① 在【开始】菜单中选择【管理工具】|【Internet 信息服务(IIS)管理器】命令，打开【Internet 信息服务(IIS)管理器】窗口。

② 右击要使用 SSL 的网站，在弹出的快捷菜单中选择【属性】命令，打开【属性】对话框。切换到【目录安全性】选项卡，在【安全通信】选项组中单击【服务器证书】按钮，如图 3-28 所示。

③ 打开【Web 服务器证书向导】对话框，单击【下一步】按钮。

④ 打开【IIS 证书向导】对话框，选择为网站分配证书的方法。这里选中【新建证书】单选按钮，单击【下一步】按钮，如图 3-29 所示。



图 3-28 【服务器证书】对话框



图 3-29 【服务器证书】界面

⑤ 打开【延迟或立即请求】界面，选中【现在准备证书请求，但稍后发送】单选按钮，单击【下一步】按钮。

⑥ 打开【名称和安全性设置】界面，在【名称】文本框中输入新证书的名称，在【位长】下拉列表框中选择密钥的位长，如图 3-30 所示。

⑦ 打开【单位信息】界面，输入单位和部门的名称，单击【下一步】按钮。

⑧ 打开【站点公用名称】界面，输入站点的公用名称，单击【下一步】按钮。

⑨ 打开【地理信息】界面，输入的地理信息包括国家、省/自治区、市县，单击【下一步】按钮。

⑩ 打开【证书请求文件名】界面，输入证书请求的文件名，以指定的文件名将证书请求保存为文本文件，单击【下一步】按钮。



图 3-30　【名称和安全性设置】界面

⑪ 打开【请求文件摘要】界面，显示请求文件包含的信息。单击【下一步】按钮，证书请求创建完毕。

第三步：提交数字证书申请。

① 在服务器的 IE 浏览器中输入地址：http://localhost/CertSrv/default.asp，打开【Microsoft 证书服务】欢迎页面，如图 3-31 所示。单击【申请一个证书】超链接。

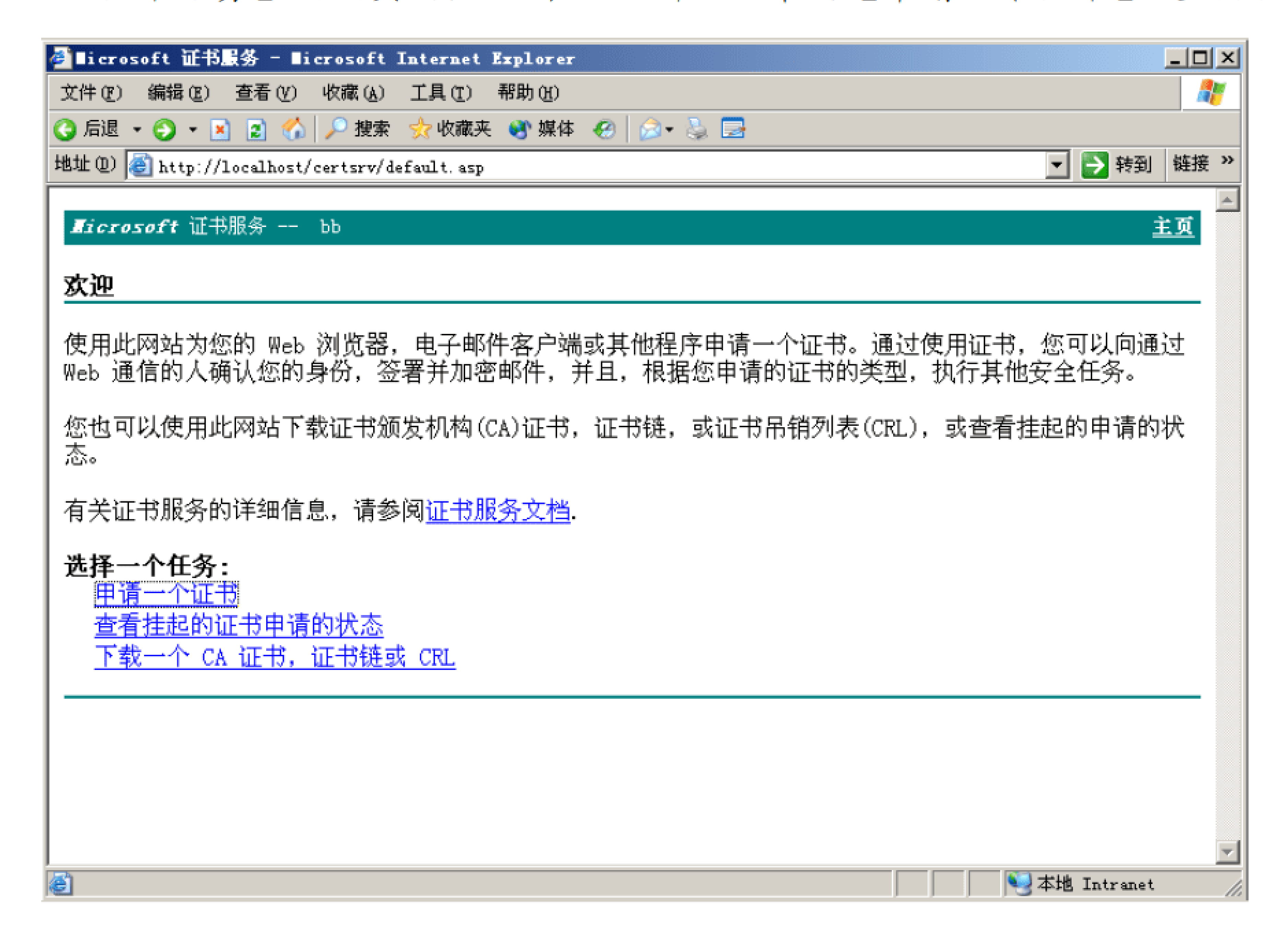
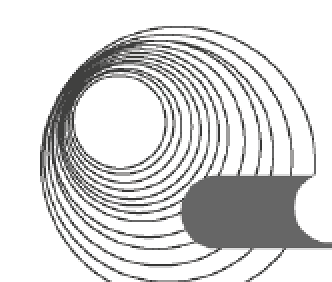


图 3-31　【Microsoft 证书服务】欢迎页面

② 打开【申请一个证书】页面，如图 3-32 所示，选择证书申请类型，这里单击【高级证书申请】超链接。



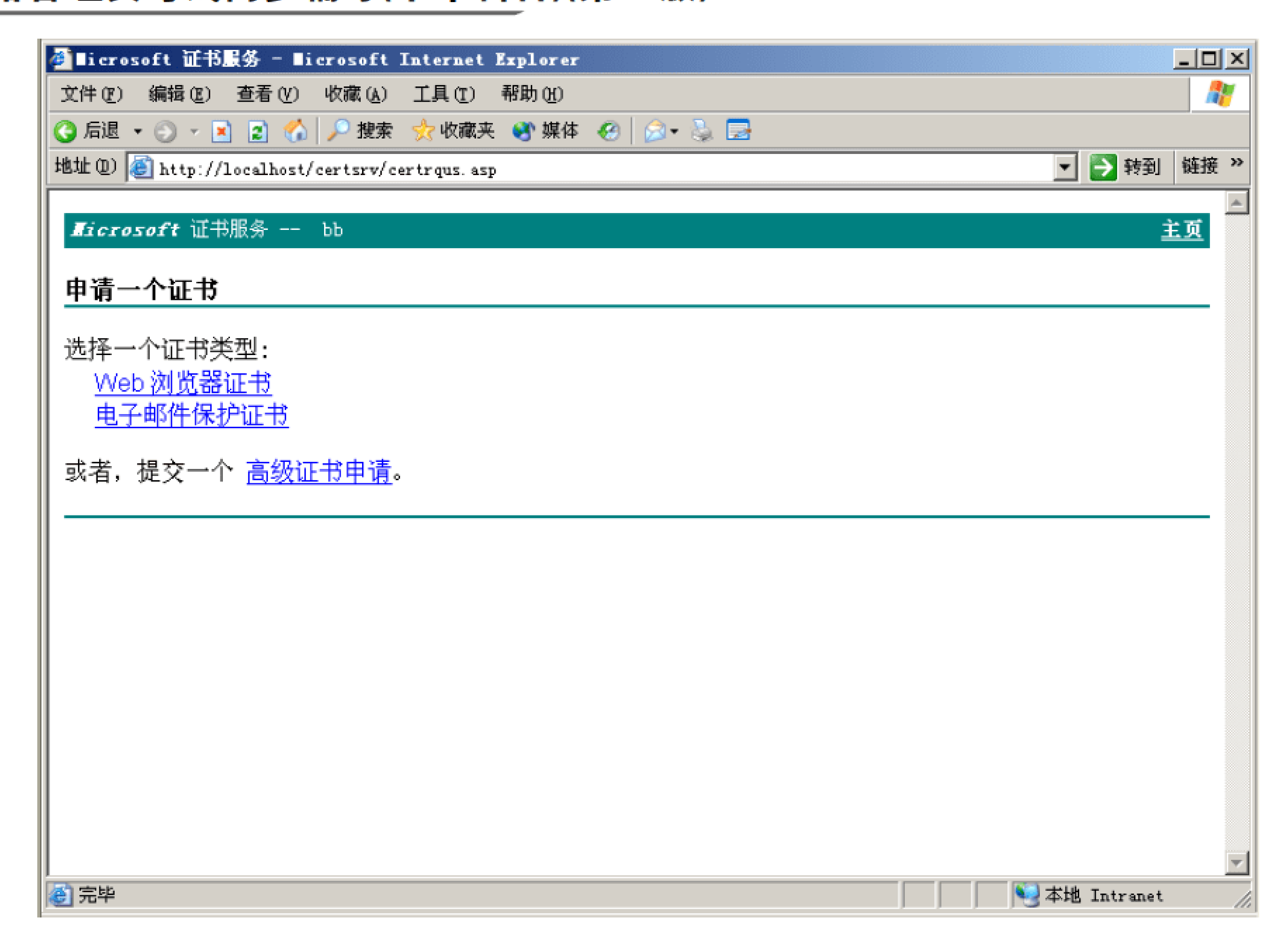


图 3-32 【申请一个证书】页面

③ 打开【高级证书申请】页面，如图 3-33 所示，选择 CA 策略，这里单击【使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请】超链接。

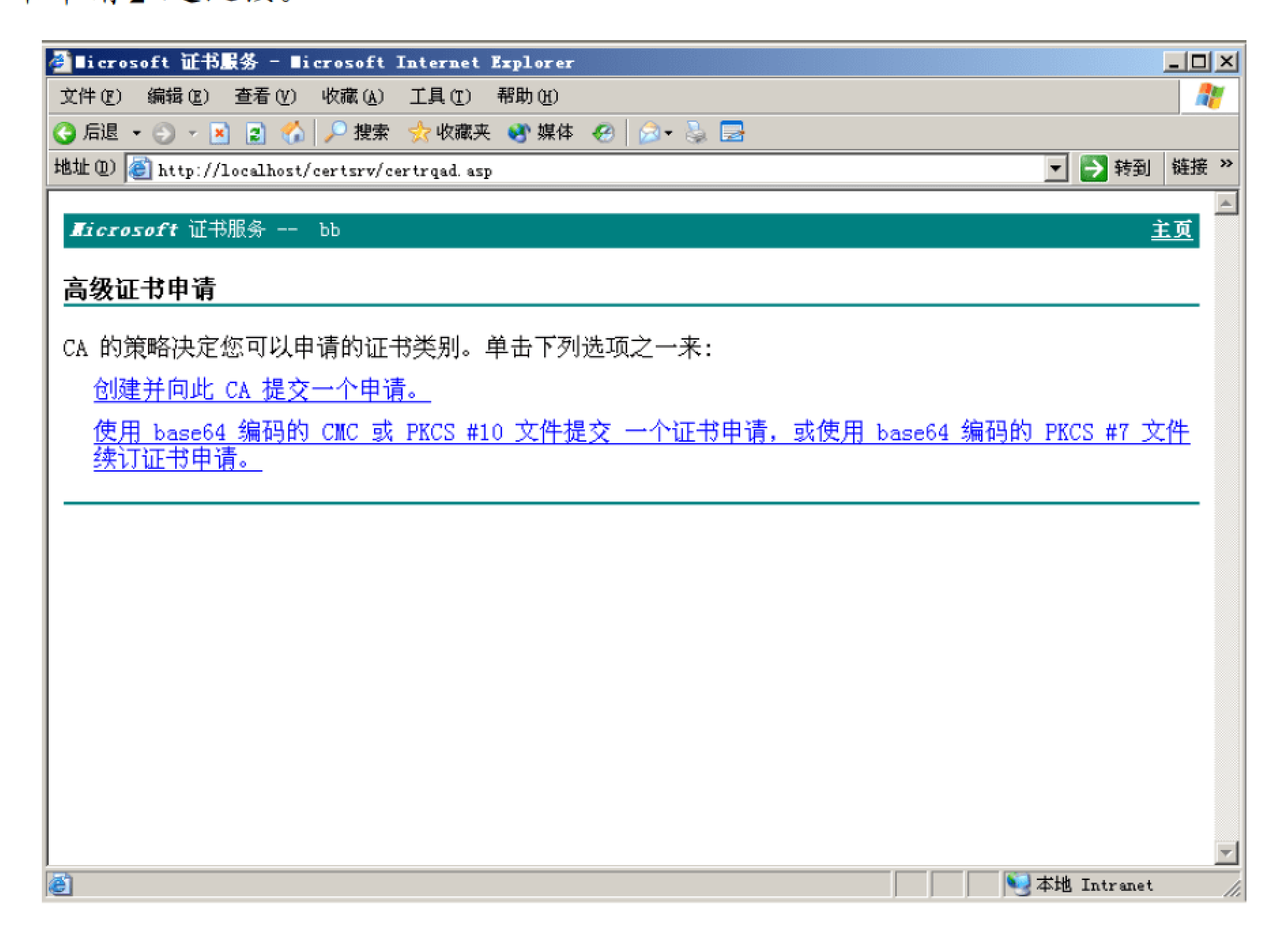


图 3-33 【高级证书申请】页面

④ 打开【提交一个证书申请或续订申请】页面，如图 3-34 所示。然后打开步骤(2)中生成的 certreq.txt 文件，复制其中的内容到【保护的申请】文本区域，单击【提交】按钮。

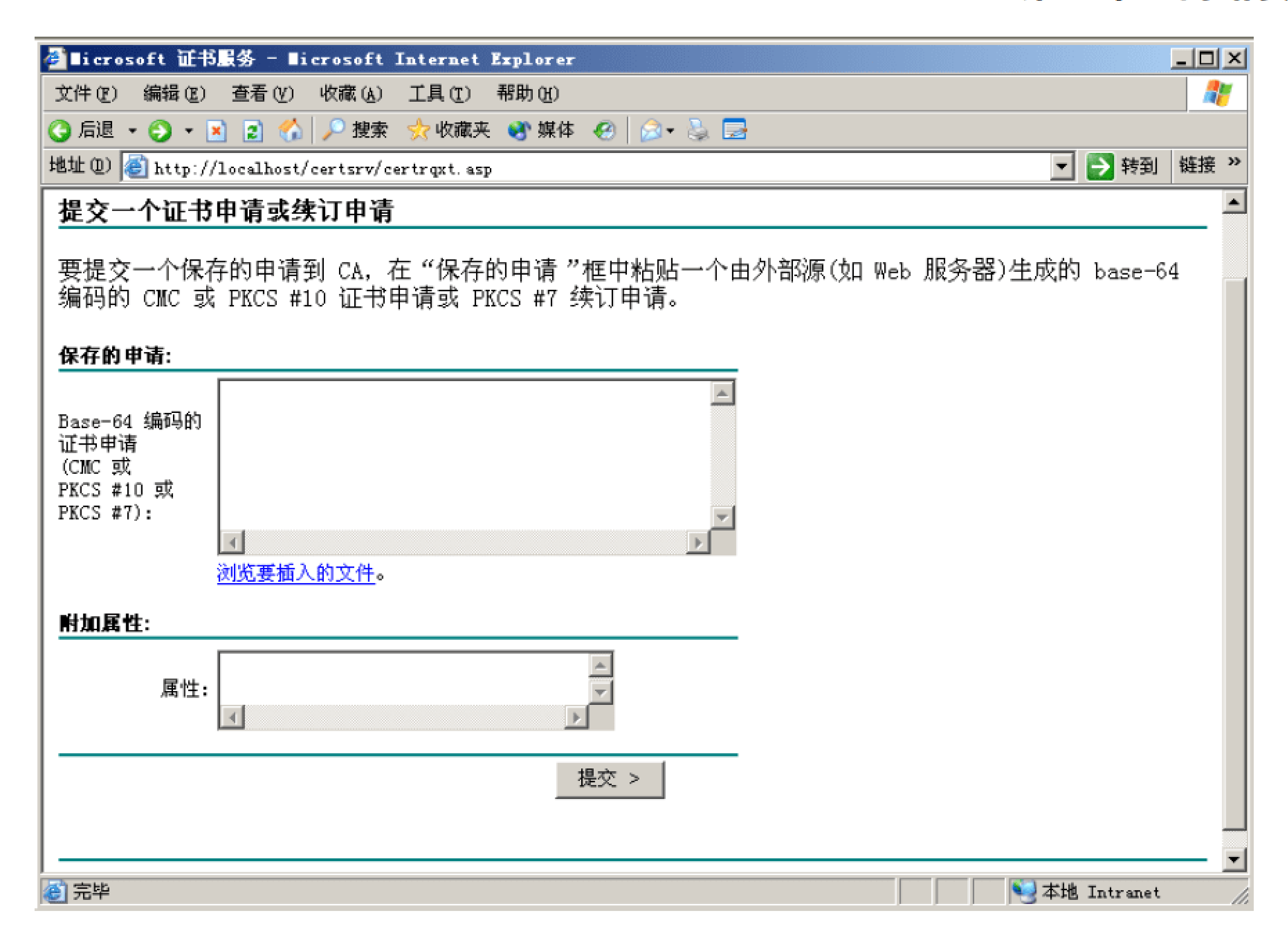


图 3-34　【提交一个证书申请或续订申请】页面

⑤　打开【证书挂起】页面，提示证书申请收到，如图 3-35 所示。

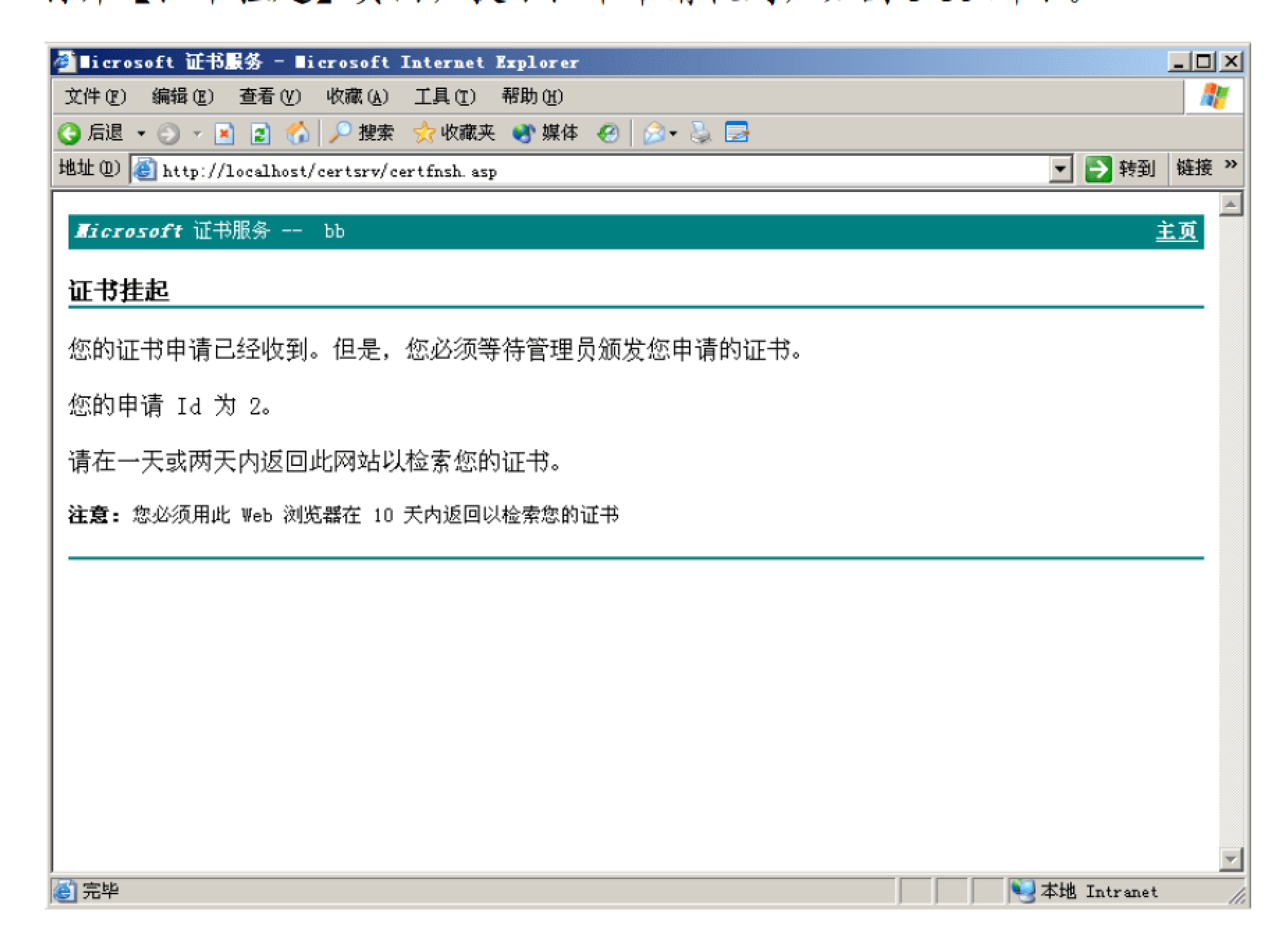


图 3-35　【证书挂起】页面

第四步：导出证书文件。

①　在【开始】菜单中选择【管理工具】|【证书颁发机构】命令，打开【证书颁发机构】窗口。在左侧窗格中展开树状目录，单击【挂起的申请】选项，在右侧窗格中找到并右击步骤(3)中申请的证书，在弹出的快捷菜单中选择【所有任务】|【颁发】命令，如图 3-36

所示。

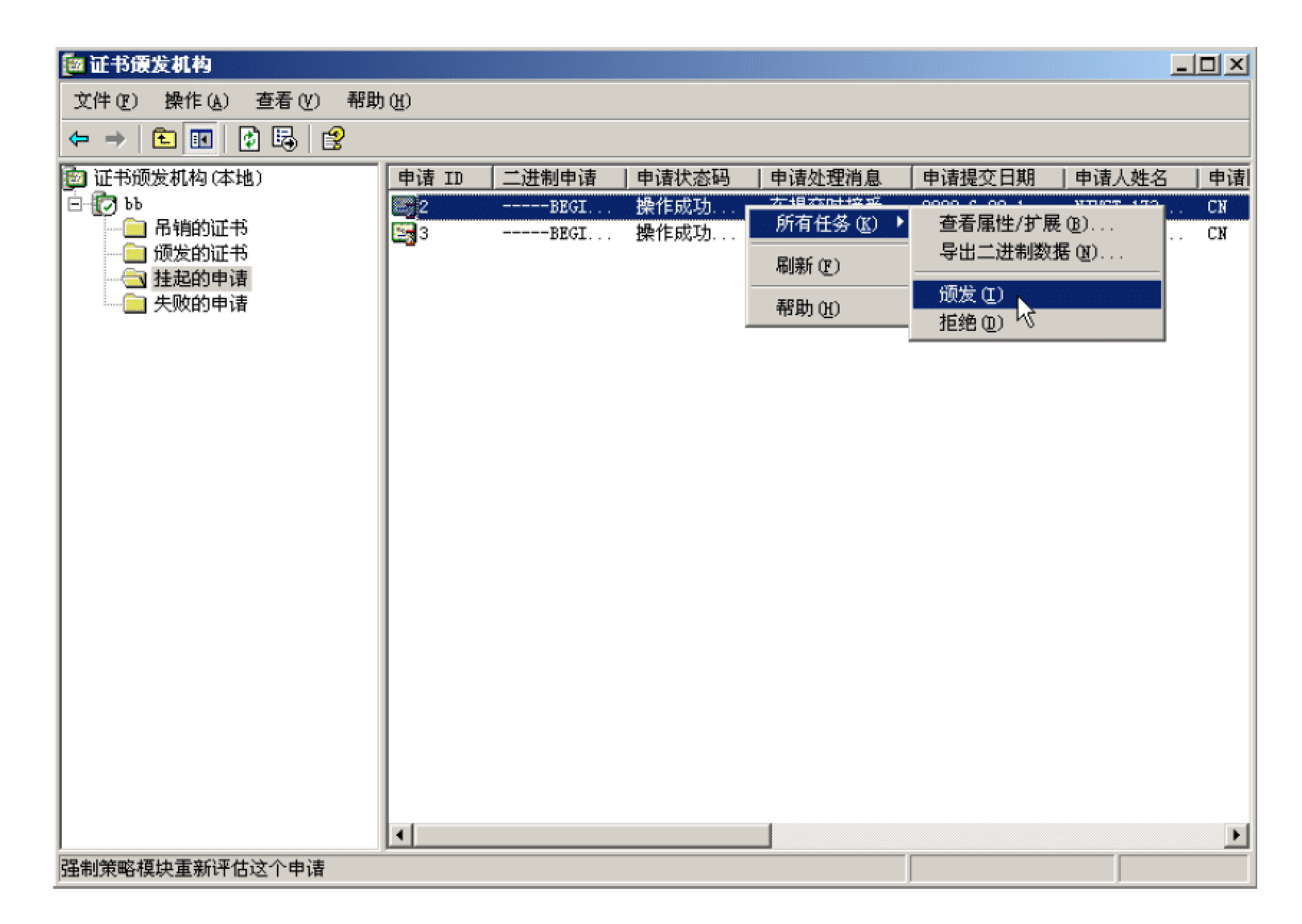


图 3-36 【证书颁发机构】窗口

② 颁发成功后，单击左侧窗格中的【颁发的证书】选项，可以看到刚刚颁发的证书。双击该证书，弹出【证书】对话框。切换到【详细信息】选项卡，单击【复制到文件】按钮，如图 3-37 所示。

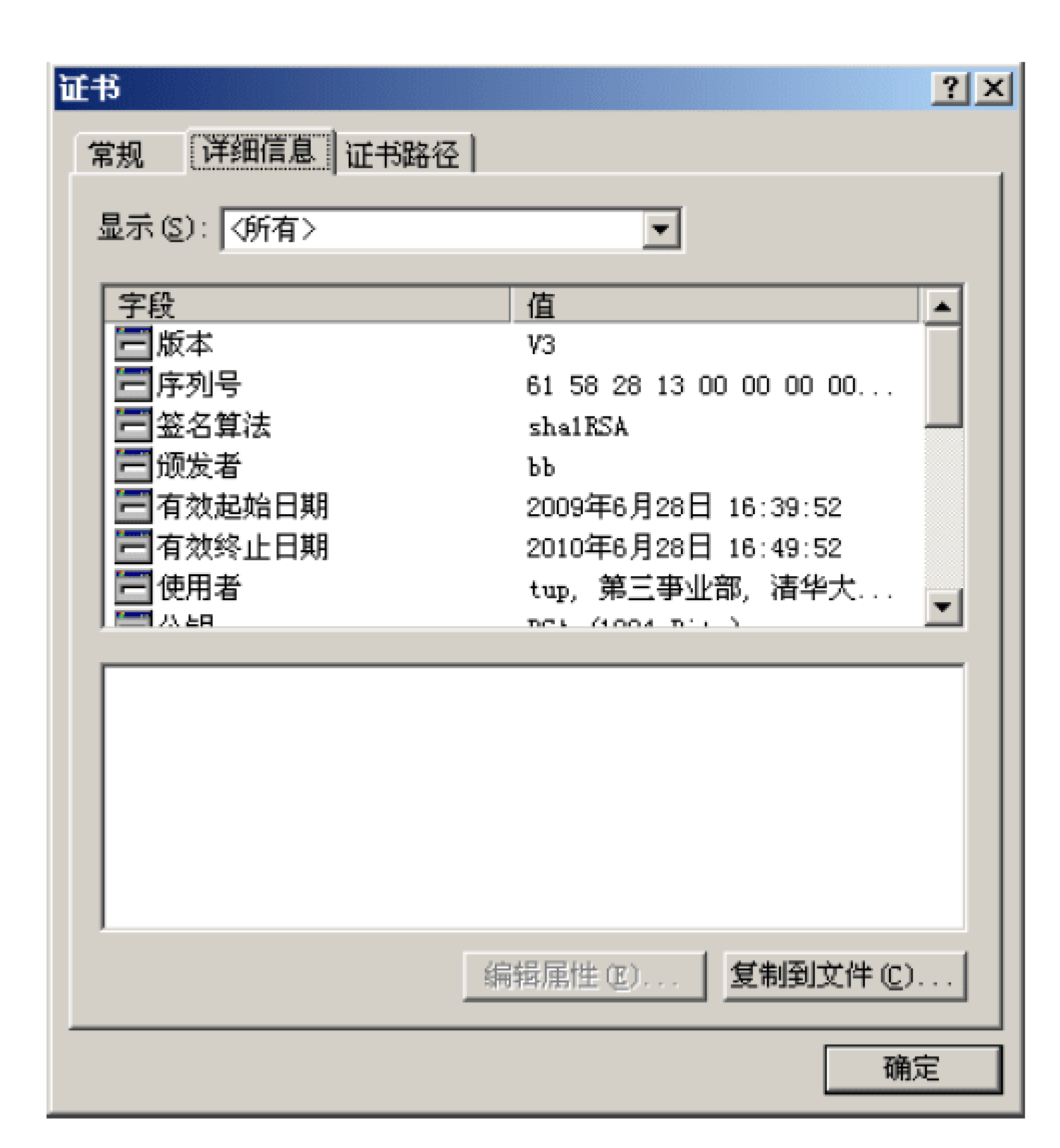


图 3-37 【证书】对话框

③ 弹出【证书导出向导】对话框，如图 3-38 所示。单击【下一步】按钮，打开【导出文件格式】对话框，选择导出证书要使用的格式。单击【下一步】按钮，打开【要导出的文件】对话框，指定要导出的文件名。单击【下一步】按钮，证书导出完成，如图 3-39 所示。

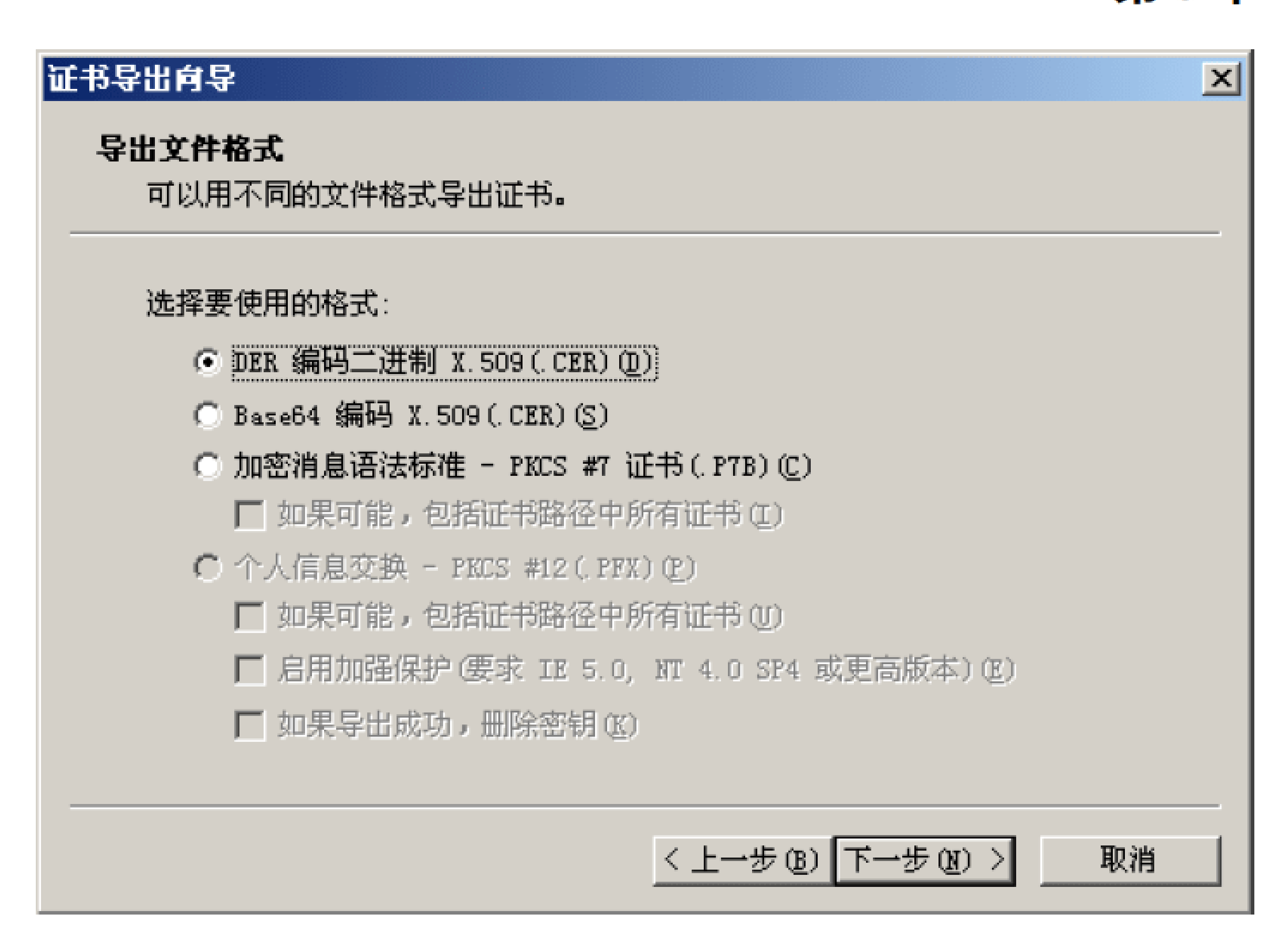


图 3-38　【证书导出向导】对话框

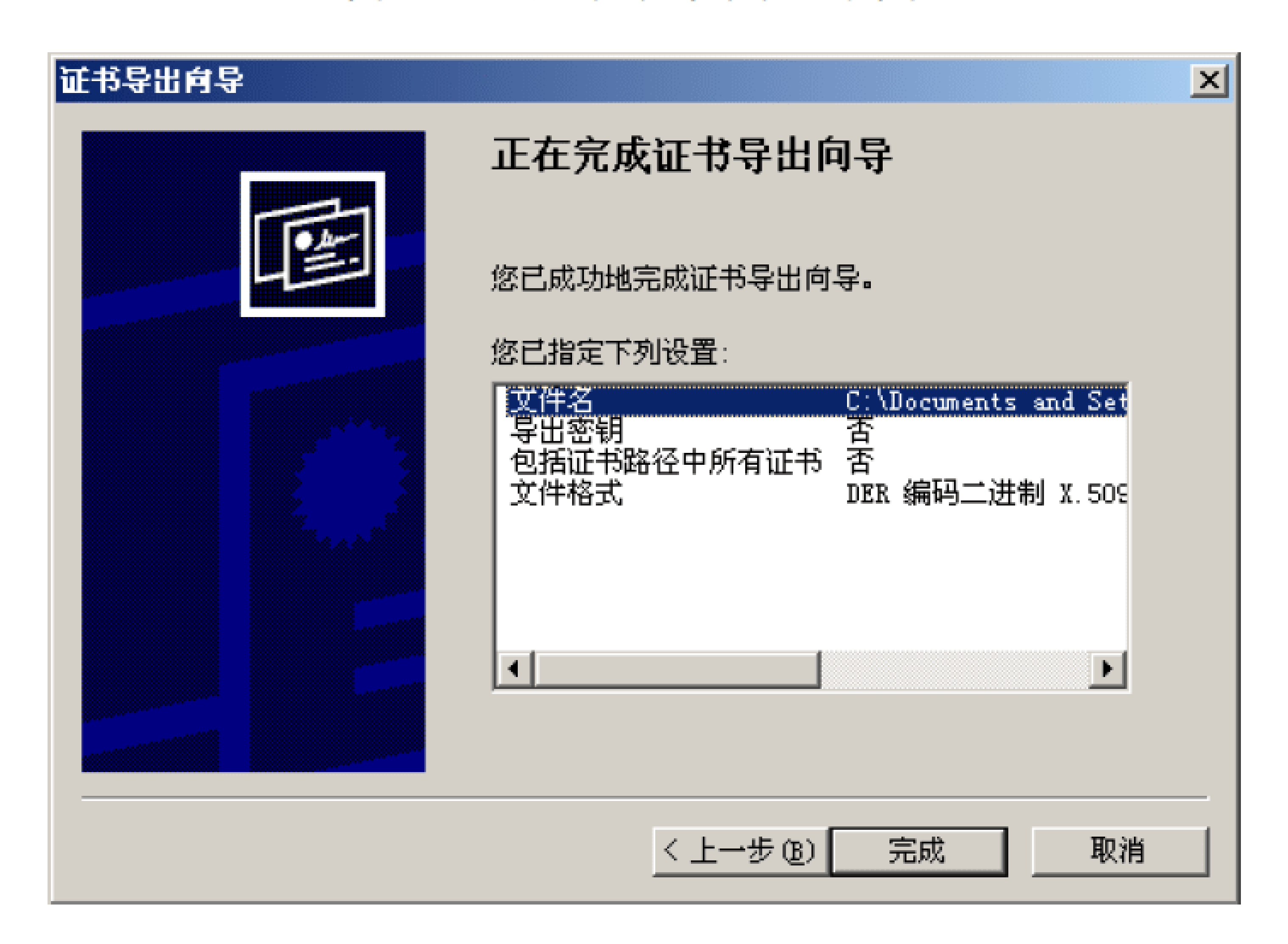


图 3-39　完成证书导出

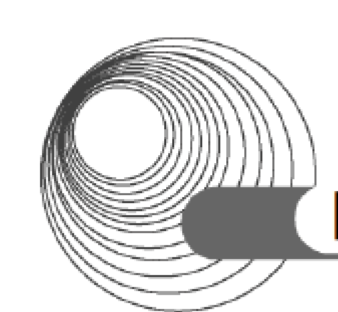
第五步：在 IIS 服务器上安装证书。

① 返回【Internet 信息服务(IIS)管理器】窗口，右击要使用 SSL 的网站，在弹出的快捷菜单中选择【属性】命令，打开【属性】对话框。切换到【目录安全性】选项卡，在【安全通信】选项组中单击【服务器证书】按钮，打开【Web 服务器证书向导】对话框。单击【下一步】按钮，打开【挂起的证书请求】界面，选中【处理挂起的请求并安装证书】单选按钮，单击【下一步】按钮，如图 3-40 所示。

② 打开【处理挂起的请求】界面，设置服务器证书文件的位置和文件名，单击【下一步】按钮，如图 3-41 所示。

③ 打开【SSL 端口】界面，为网站指定 SSL 端口，单击【下一步】按钮，如图 3-42 所示。

④ 打开【证书摘要】对话框，显示证书详细信息，单击【下一步】按钮完成安装。



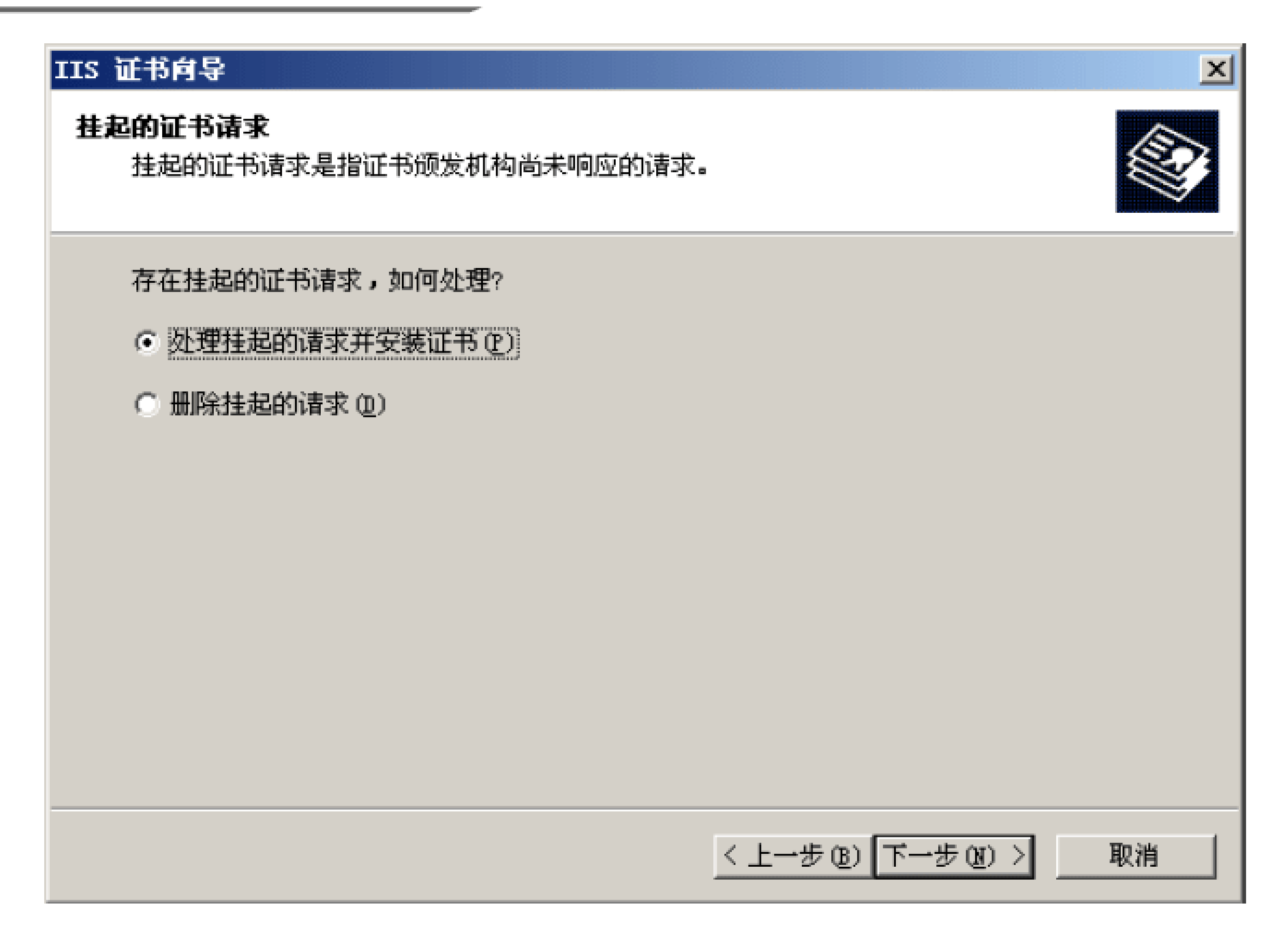


图 3-40 【挂起的证书请求】界面

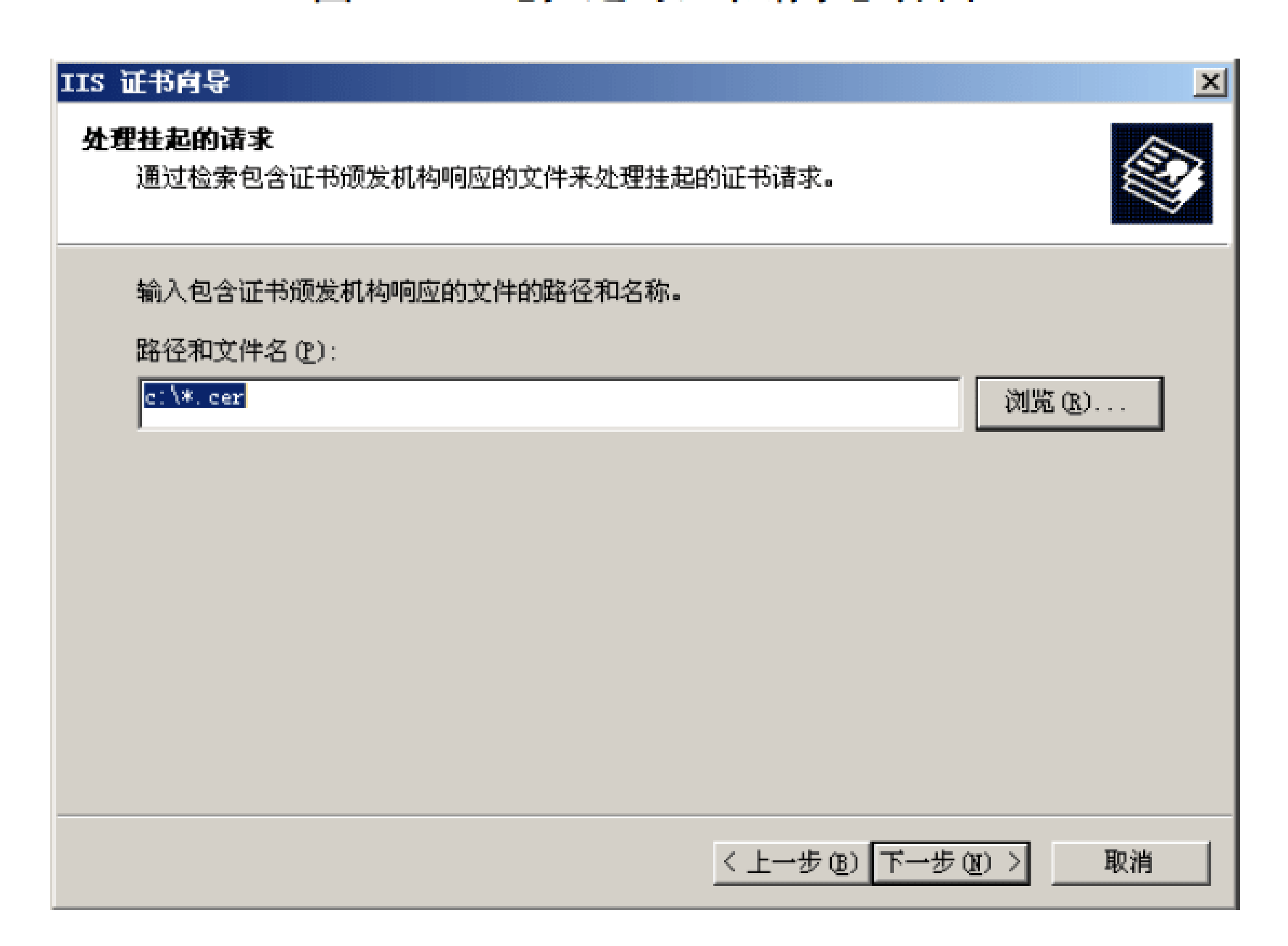


图 3-41 【处理挂起的请求】界面

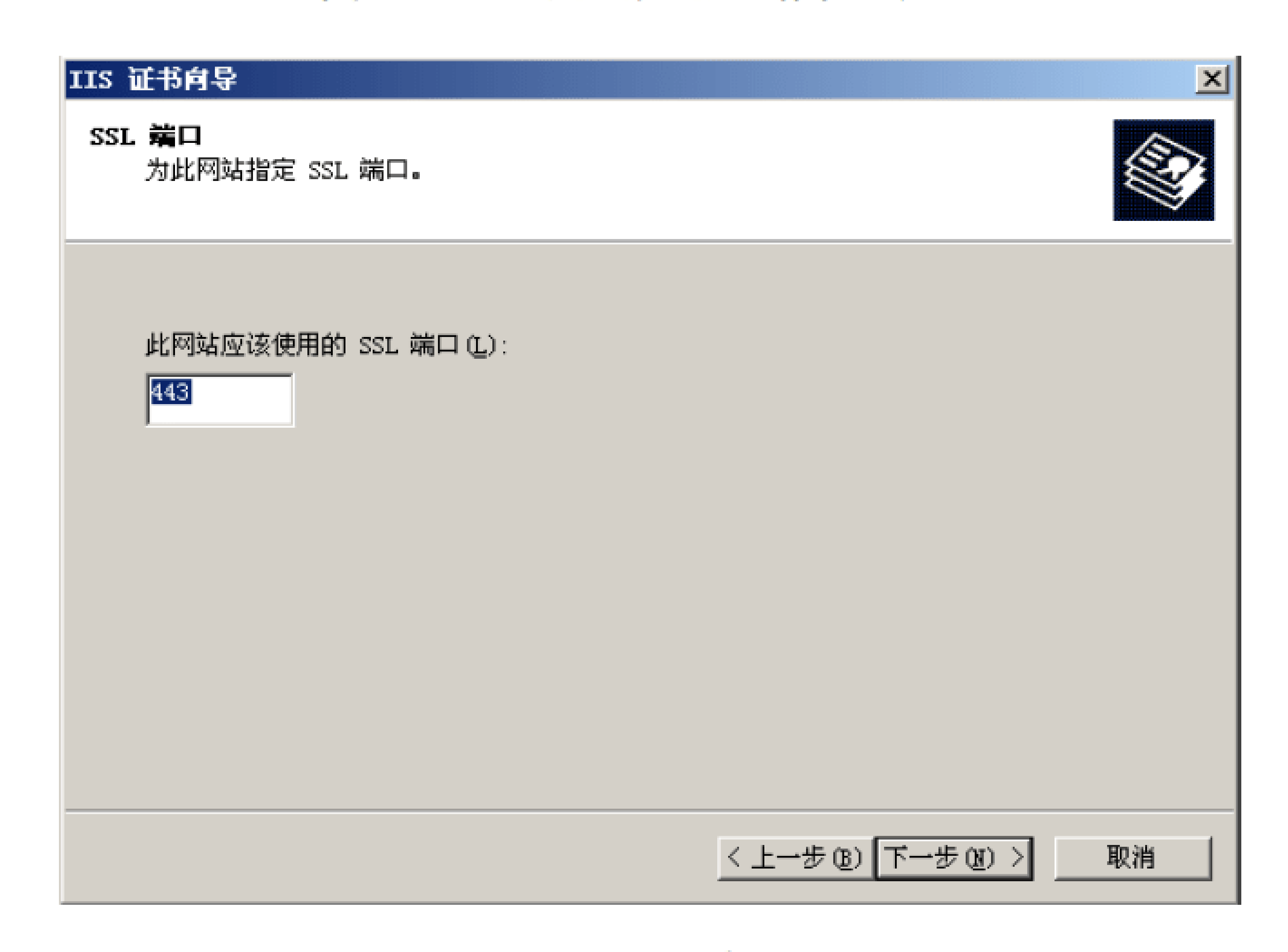


图 3-42 【SSL 端口】界面

第六步：配置身份验证方式和 SSL 安全通道。

在【安全通信】选项组中单击【编辑】按钮，打开【安全通信】对话框。选中【要求安全通信(SSL)】复选框，单击【确定】按钮即可启用 SSL，如图 3-43 所示。

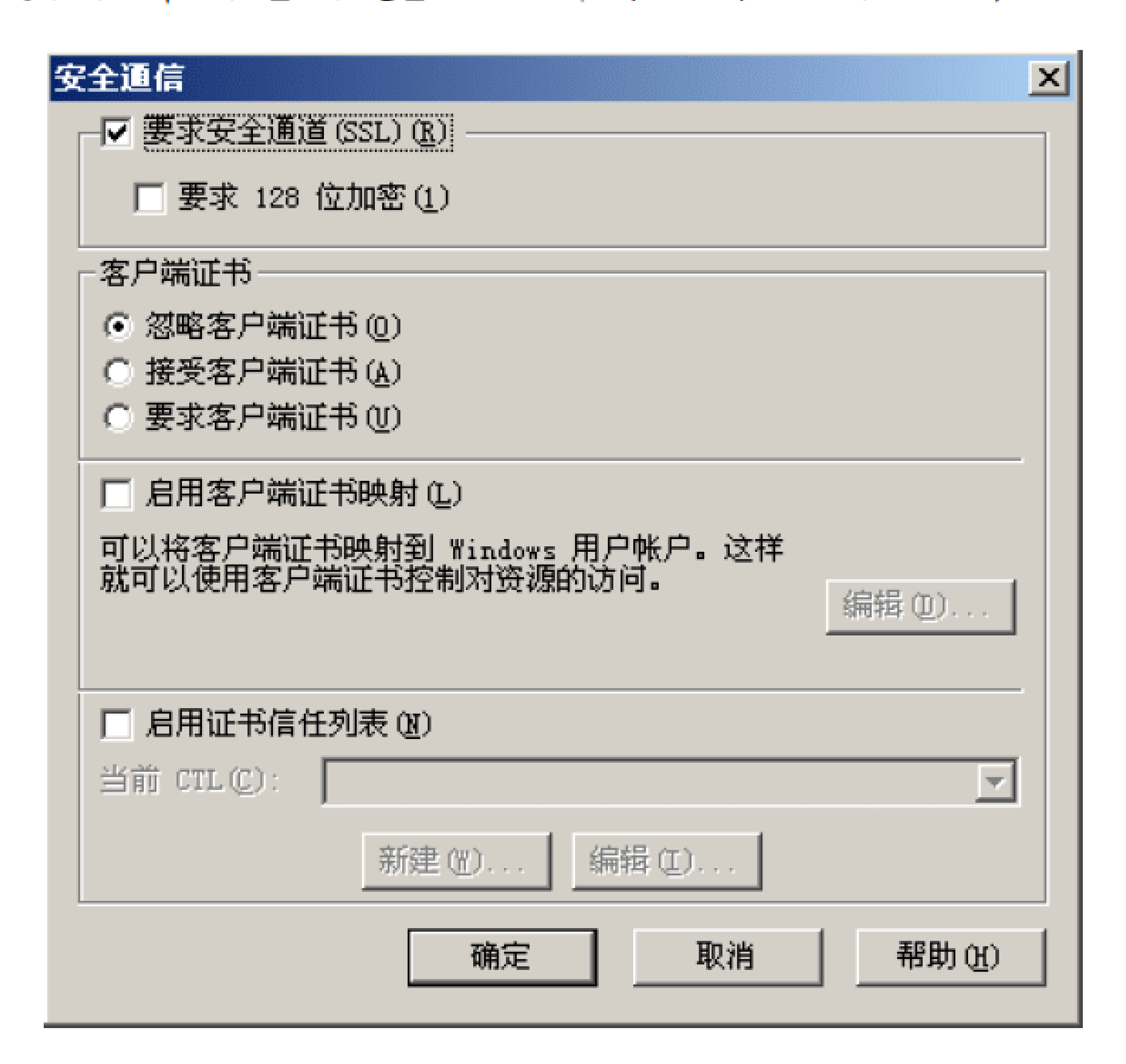


图 3-43　【安全通信】对话框

【问题 4】在【安全通信】对话框中，选中【要求安全通道(SSL)】和【要求 128 位加密】复选框，选中【忽略客户端证书】单选按钮。

【问题 5】用户只要在 IE 浏览器中输入 https://网站地址就可以访问该网站。本题中的 IP 地址为 211.120.114.3，端口号为 8080，因此输入 https://211.120.114.3:8080 就可以通过 SSL 安全通道访问该 Web 网站。

答案：

【问题 1】

(1) B　　　　(2) C

注：(1)与(2)的答案可互换。

【问题 2】

(3) C　　　　　(4) B

【问题 3】

(5) 证书认证(颁发) 机构或 CA

(6) B　　　　　(7) A　　　　　　(8) C

【问题 4】

选中【要求安全通道(SSL) 】复选框，选中【要求 128 位加密】复选框，选中【忽略客户端证书】单选按钮。

【问题 5】

(9) https://211.120.114.3:8080

3.2.3 同步练习

1. 阅读以下说明，回答问题 1～问题 3。

【说明】

某公司对外提供 Web 服务及 E-mail 和 DNS 服务等，同时对所有员工提供 Internet 服务。其拓扑结构如图 3-44 所示。

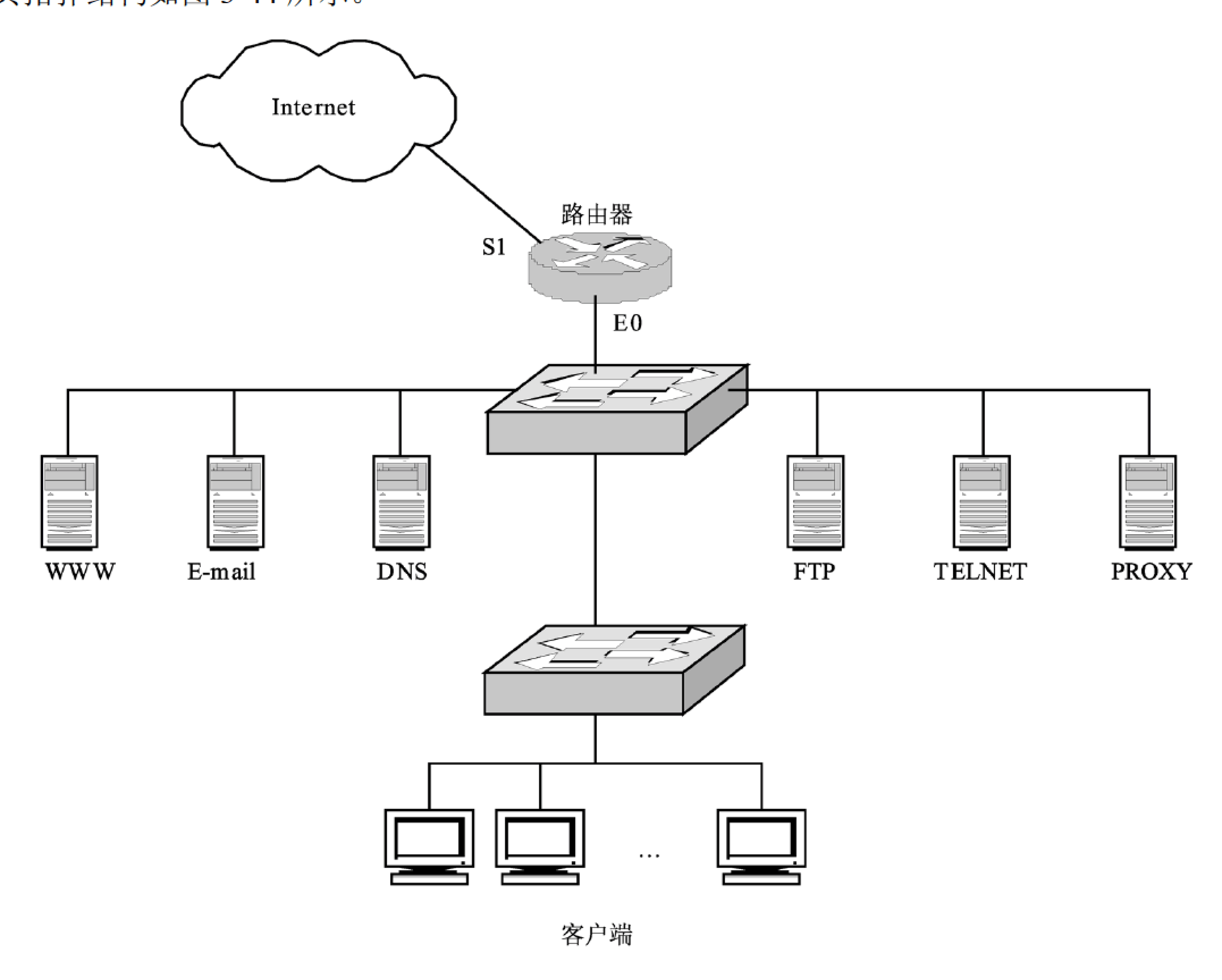


图 3-44 某公司网络拓扑结构

具体网络情况如下。

① 外网(即外部网)接口 S1，地址为 211.156.169.6/30(子网掩码表示由 30 个 1 组成，下同)，因特网接口端地址为 211.256.169.5/30。

② 内网(即内部网)接口 E0，地址为 210.45.12.1/24(可用地址空间为 210.45.12.0～210.45.12.255 这个网段，广播地址为 210.45.12.255)。

③ 对外服务器默认网关为 210.45.12.1。

④ 内网用户利用代理服务上网(代理服务器 IP 地址为 210.45.12.31/24)。

⑤ 内网用户 IP 地址为 210.45.12.0 网段，子网掩码为 255.255.255.0，网关为 210.45.12.1，代理服务器地址为 210.45.12.31。

随着用户的增多，IP 地址紧缺的矛盾日益突出，同时内部网用户及服务器常遭受黑客的攻击。为解决上述问题，公司决定购置一台方正防火墙。

【问题 1】请给出具体方案(拓扑图)。

【问题 2】简述防火墙的硬件连接。

【问题 3】简述防火墙的配置策略。

2. 图 3-45 所示为某一公司的网络拓扑结构，请在图中标出公共网络、内部网络、DMZ 区、内部关键服务器群的位置。

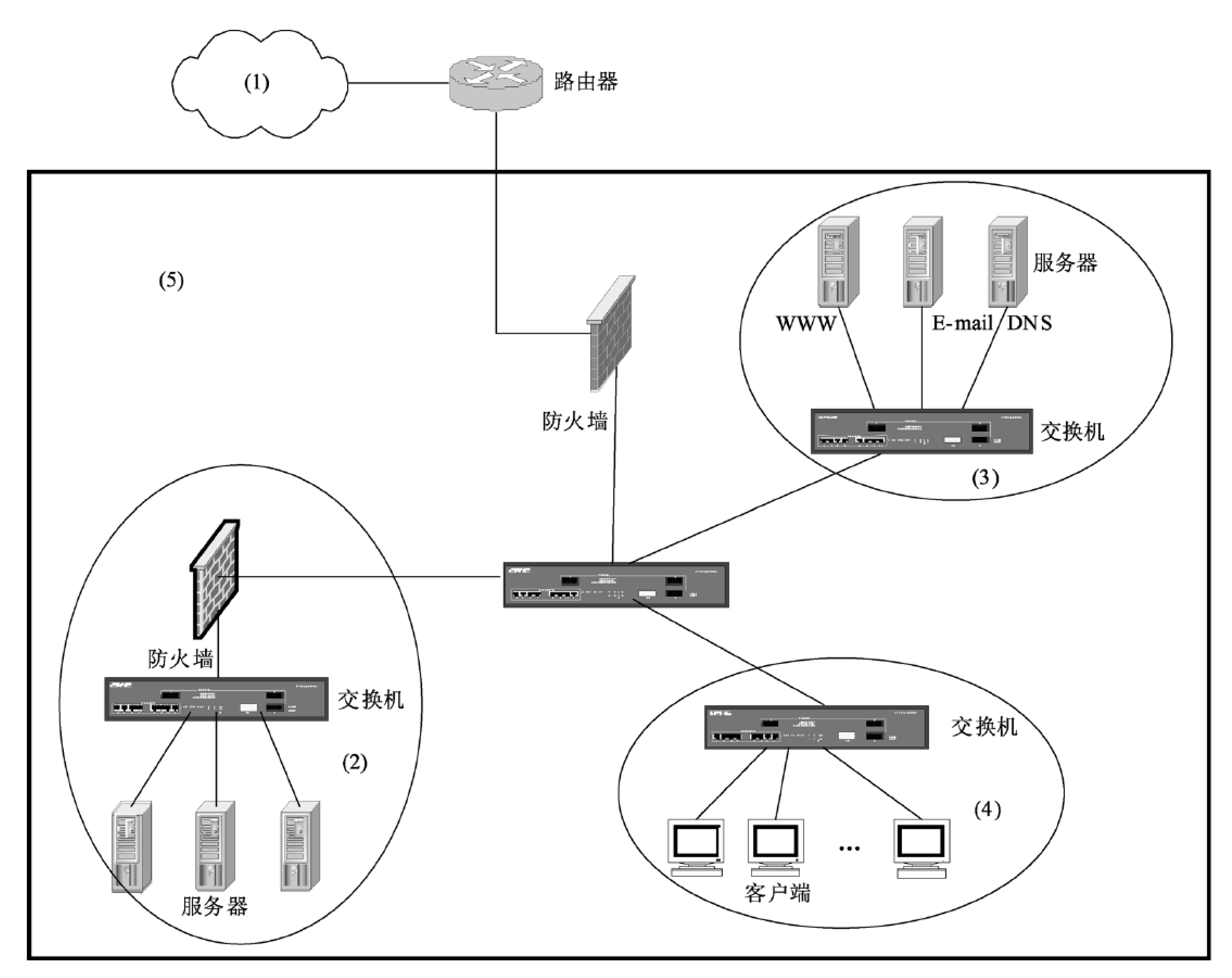


图 3-45　某公司网络拓扑结构

3.2.4　同步练习参考答案

1.

【问题 1】其连接拓扑结构如图 3-46 所示。

【问题 2】硬件连接如下。

- 用网线将路由器 E0 端口与 FireGate 的外部接口相连。
- 用网线将内部交换机端口与 FireGate 的内部接口相连。
- 用网线将 DMZ 接口与 DMZ 区交换机相连。
- 用电源线将 FireGate 接上电源，硬件安装完成。

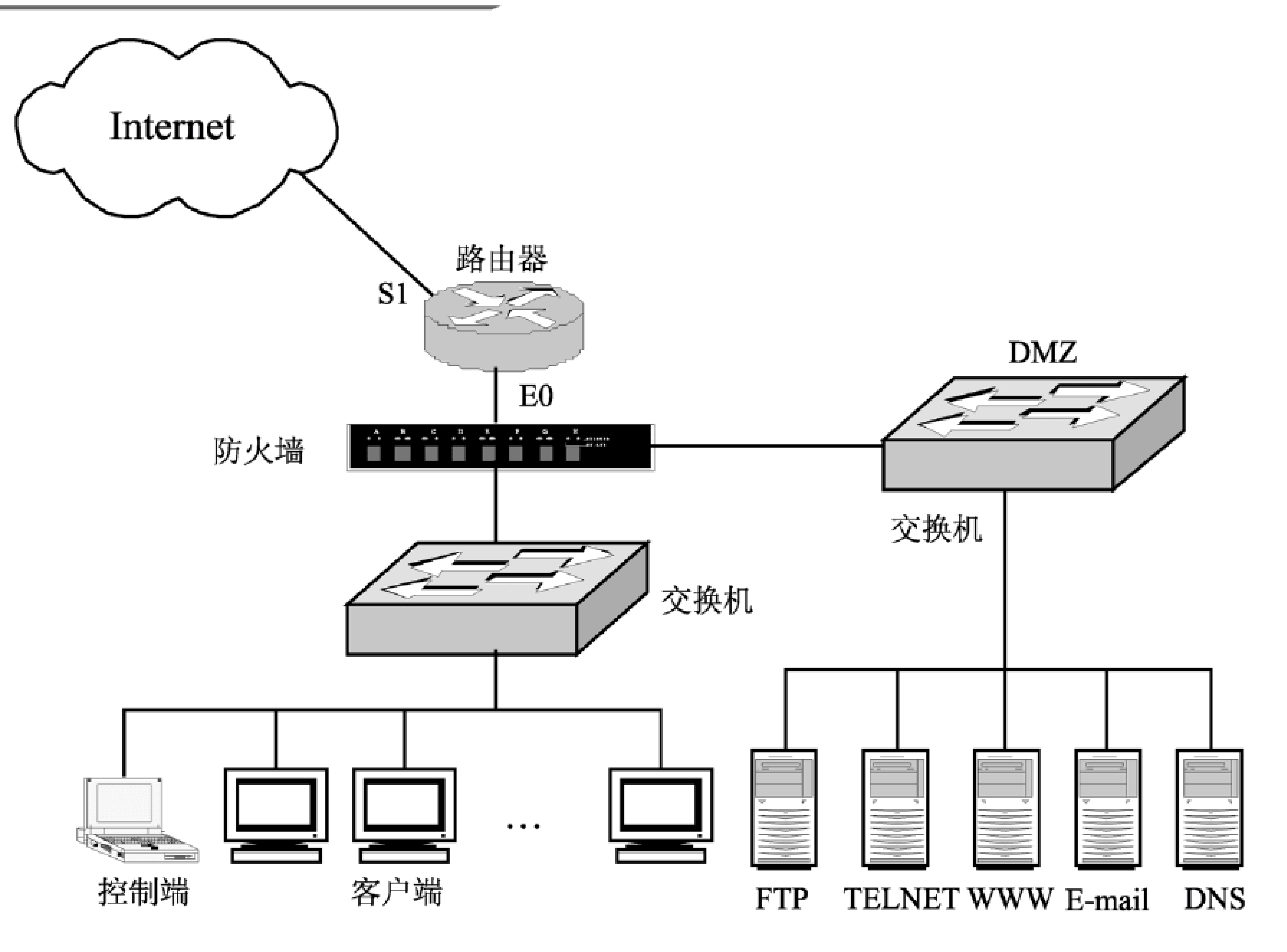


图 3-46　接入防火墙后的网络拓扑

【问题 3】其配置策略如下。

① 基本配置。

- 防火墙内部接口设为防火墙内部网络接口和管理口，地址为 192.168.1.1/24，设置好相应的子网掩码后将其选为控制口，然后提交系统，使设备配置生效。
- 将 DMZ 区域和外网区域设置为桥，同时在桥上绑定 IP 地址 210.45.12.31/24(为原代理服务器地址)，配置完成后提交系统，使设备配置生效。
- 添加内部网、DMZ 区域以及外部网各设备别名。

② 规则配置。

- 按照实际情况配置各种安全措施，如内部网访问 DMZ 区域 Web 服务器规则，内部网访问 DMZ 区域 Telnet 服务器规则等。
- NAT 规则设置。在防火墙设置 NAT 功能实现地址转换，内部网访问外部 WWW 时，全部将内部地址转换成防火墙外部网地址 210.45.12.31，不需要代理服务器。

2.

① 公共网络或 Internet

② 内部关键服务器群区

③ DMZ 区

④ 一般用户区

⑤ 内部网络

3.3　本 章 小 结

本章知识点在 2009 年的新大纲中变化较小，主要新增了加密、认证、数字签名等安全技术知识点。

本章主要介绍了网络病毒防护策略、防火墙的配置策略、入侵处理策略。要求考生掌握网络病毒防护、防火墙、入侵处理的基本概念，熟悉在不同网络环境下的部署及网络安全解决方案。

本章内容为下午科目的重点内容，尤其是防火墙的配置，曾多次考到。

3.4　达标训练题及参考答案

3.4.1　达标训练题

阅读以下说明，回答问题 1～问题 4。

【说明】

某学校的拓扑结构如图 3-47 所示，为加强网络安全，学校决定购置一台三端口的防火墙保护内部网络；购置了入侵检测产品对重点网段和服务器进行监控；购置一套网络版杀毒软件(Server 版)并安装于一台服务器上，客户端、服务器通过防病毒服务器提供的 Web 页面自动下载安装并具有自动跟踪防病毒服务器更新病毒库的功能。

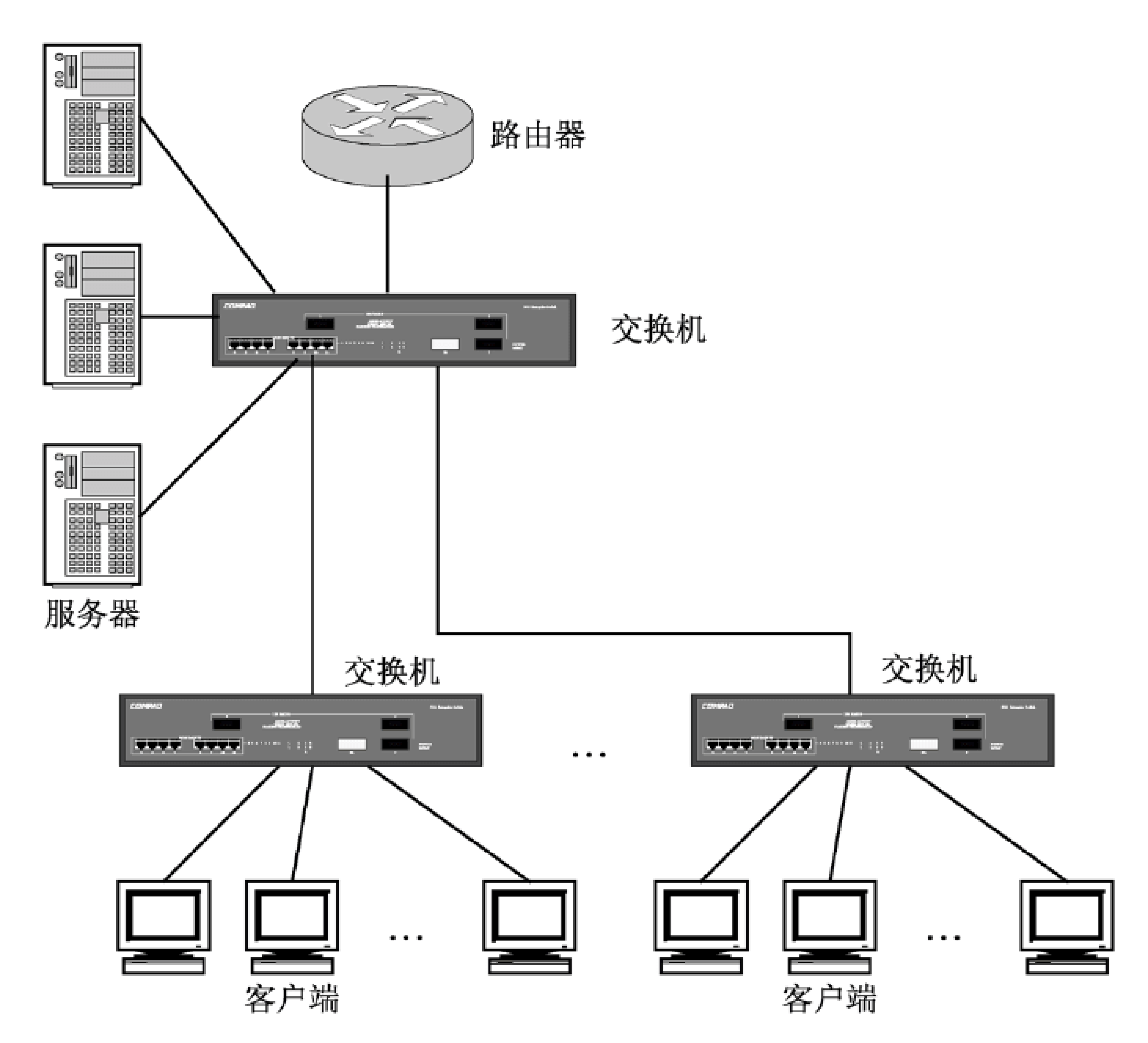


图 3-47　某校园网拓扑结构

【问题 1】什么是防火墙？简述其功能及优点。

【问题 2】什么是入侵检测？简述其功能。

【问题 3】什么是网络病毒？简述其特点。对防病毒服务有什么要求？

【问题 4】请给出该网络的安全方案(拓扑结构图)，并在图中标出相应设备的名称。

3.4.2 参考答案

【问题 1】防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。其功能与特点如下。

- 对进出的数据包进行过滤，过滤掉不安全的服务和非法用户。
- 监视 Internet 安全，对网络攻击行为进行检测和报警。
- 记录通过防火墙的信息内容和活动。
- 控制对特殊站点的访问，封堵某些禁止的访问行为。
- 防火墙能强化安全策略。
- 防火墙能有效地记录 Internet 上的活动。
- 防火墙是一个安全策略的边防站。

【问题 2】入侵检测系统(IDS)通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统可以说是防火墙系统的合理补充和延伸，如果说防火墙是第一道安全闸门，入侵检测系统则可以说是第二道安全闸门。入侵检测系统在不影响网络性能的前提下，可实时、动态地保护来自内部和外部的各种攻击，同时有效地弥补了防火墙所能达到的防护极限。入侵检测系统的主要功能如下。

- 监测并分析用户和系统的活动。
- 核查系统配置和漏洞。
- 评估系统关键资源和数据文件的完整性。
- 识别已知的攻击行为。
- 统计分析异常行为。
- 进行操作系统日志管理，并识别违反安全策略的用户活动。

【问题 3】网络病毒是指在网络上传播的计算机病毒，可能会给网络带来灾难性后果，被称为“第二代病毒”。网络病毒的特点及危害性主要表现在：破坏性强、传播性强、具有潜伏性和可激发性、针对性更强、扩展面广、传播速度快、难以彻底清除的特点。

要求防病毒服务器每天下载并更新病毒定义库。

【问题 4】其配置拓扑结构如图 3-48 所示。

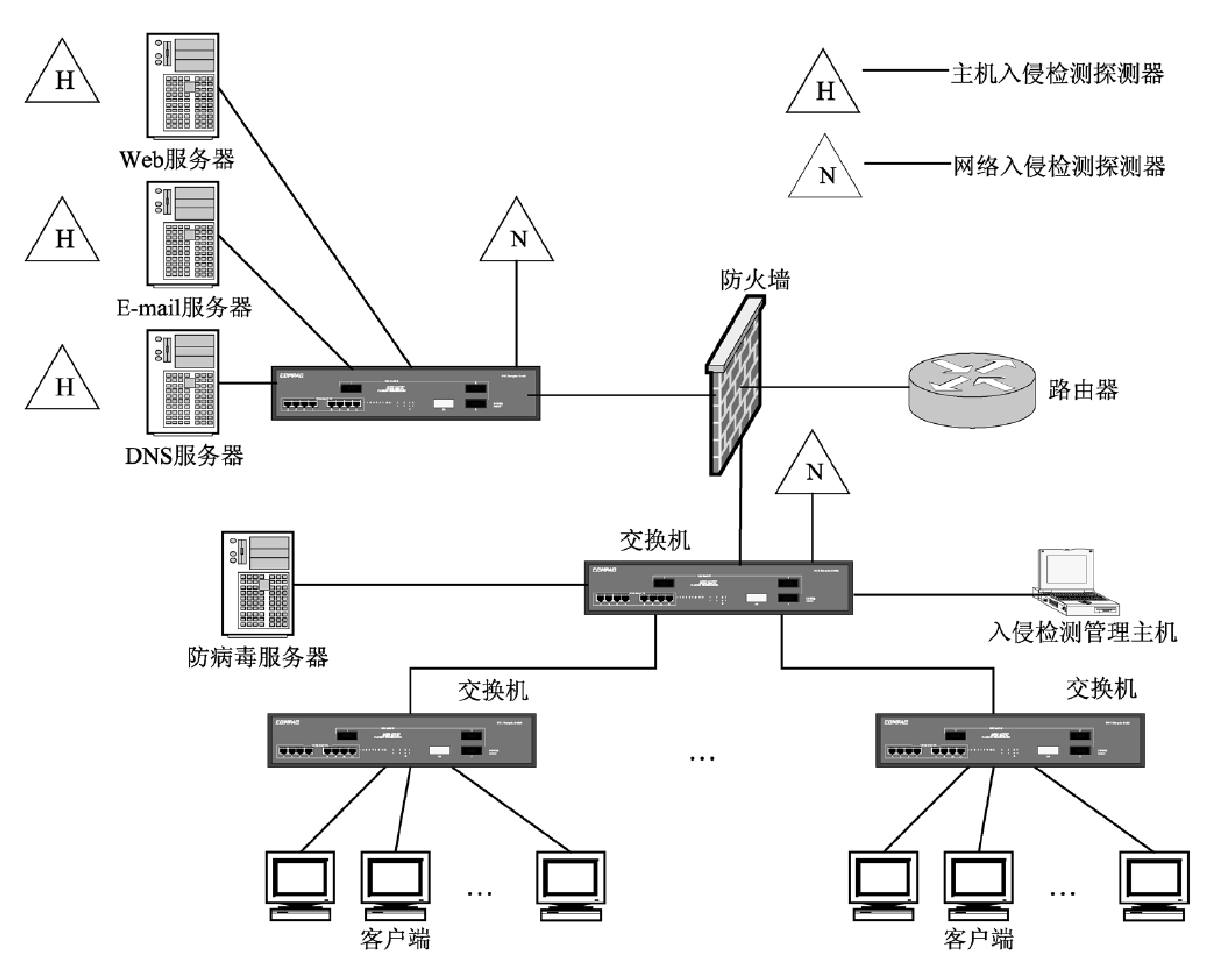


图 3-48　解决网络安全的拓扑结构

第 4 章　网络管理与故障处理

大纲要求：

- 使用网络管理软件对网络的配置、安全、性能、故障、计费进行监督和管理
- 简单网络故障的分析、定位、诊断和排除
- 小型网络的维护策略、计划和实施
- 数据备份和数据恢复
- 系统性能分析

4.1　网络管理软件

4.1.1　考点辅导

4.1.1.1　网络管理系统

当前能够作为管理进程运行的典型的网络管理软件有：惠普公司的 OpenView、IBM 公司的 NetView、SUN 公司的 SunNet 以及 Cabletron 公司的 SPECTRUM。这些网络管理系统在支持企业网络管理方案的同时，也支持通过 SNMP 对网络对象进行管理。

SNMP 操作仅支持对管理对象值的检索和修改等简单操作。具体来讲，支持以下 4 种操作。

- get：用于获取特定对象的值，提取指定的网络管理信息。
- get-next：通过遍历 MIB 树获取对象的值，提供扫描 MIB 树和依次检索数据的方法。
- set：用于修改对象的值，对管理信息进行控制。
- trap：用于通报重要事件的发生，代理使用它发送非请求性通知给一个或多个预配置的管理工作站，用于向管理者报告管理对象的状态变化。

以上 4 种操作中，前 3 种是由管理者发给代理请求，需要代理发出响应给管理者；最后一种则是由代理发给管理者请求，但并不需要管理者响应。

4.1.1.2　TCP/IP 网络管理工具

网络管理工具有连接性测试程序(ping)、路由跟踪程序(tracert/trace/traceroute)、协议统计程序(netstat)和 MIB 变量浏览器。

1. ping：验证与远程计算机的连接

连接性测试程序就是 ping，它是一种最常见的网络工具，用这种工具可以测试端到端的连接性，即检查源端到目的端网络是否通畅。通过发送“Internet 控制报文协议(ICMP)”回送请求/应答报文来验证与另一台 TCP/IP 计算机的 IP 级连接。

命令格式为

```
ping IP 地址或主机名 [-t] [-a] [-n count] [-l size]
```

其中各参数含义如下。

- -t：指定在中断前 ping 可以持续发送回响请求信息到目的端。要中断并显示统计信息，可按 Ctrl+Break 组合键。要中断并退出 ping，可按 Ctrl+C 组合键。
- -a：指定对目的端 IP 地址进行反向名称解析。如果解析成功，ping 将显示相应的主机名。
- -n count：指定发送回响请求消息的次数，具体次数由 count 来指定。若不指定次数，则默认值为 4。
- -l size：指定发送的回响请求消息中“数据”字段的长度(以字节表示)。默认值为 32。size 的最大值是 65527 字节。

当计算机不能访问 Internet 时，可以首先使用 ping 命令确认是否是本地局域网的故障。假定局域网的代理服务器 IP 地址为 202.168.0.1，可使用 ping 202.168.0.1 命令查看本机是否和代理服务器连通。再测试本机的网卡是否正确安装，常用命令是 ping 127.0.0.1。

2. tracert/trace/traceroute：路由跟踪程序命令

tracert 通过递增“生存时间(TTL)”字段的值将“Internet 控制报文协议(ICMP)”回送请求/应答报文发送给目标可确定到达目标的路径。所显示的路径是源主机与目标主机间的路径中的路由器的近侧路由器接口列表。不带参数时，tracert 显示帮助。

tracert 的命令格式为

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

其中各参数含义如下。

- -d：指定不将地址解析为计算机名。
- -h maximum_hops：指定搜索目标的最大跃点数。
- -j computer-list：指定沿 computer-list 的稀疏源路由。
- -w timeout：每次应答等待 timeout 指定的毫秒数。
- target_name：目标计算机的名称或 IP 地址。

例如，想要了解自己的计算机与目标主机 www.cctv.com.cn 之间详细的传输路径信息，可以在 MS-DOS 方式下输入 tracert www.cctv.com.cn。

如果在 tracert 命令后面加上一些参数，还可以检测到其他更详细的信息。例如，使用参数-d，可以指定程序在跟踪主机的路径信息时，同时也解析目标主机的域名。

3. netstat：协议统计程序

netstat 工具是用来显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)。使用时如果不带参数，netstat 显示活动的 TCP 连接。

netstat 命令格式为

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中各参数含义如下。

- –a：显示所有连接和侦听端口。服务器连接通常不显示。
- –e：显示以太网统计。该参数可以与-s 选项结合使用。
- –n：以数字格式显示地址和端口号(而不是尝试查找名称)。
- –s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。
- –p protocol：显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp，如果与 -s 选项一起使用显示每个协议的统计，则 protocol 可以是 tcp、udp、icmp 或 ip。
- –r：显示路由表的内容。
- interval：重新显示所选的统计，在每次显示之间暂停 interval 秒。按 Ctrl+B 组合键停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

4. MIB 变量浏览器

MIB 变量浏览器是另一种重要的网络管理工具。在 SNMP 中，MIB 变量包含了路由的几乎所有重要参数。对路由器进行管理，很大程度上是利用 MIB 变量来实现的。比如，路由器的路由表、路由器的端口流量数据、路由器中的计费数据、路由器 CPU 的温度、负载以及路由器的内存余量等，所有这些数据都是从路由器的 MIB 变量中采集到的。虽然对 MIB 变量的定时采集与分析，大部分都是程序进行的，但一种图形界面下的 MIB 变量浏览器也是需要的。一般 MIB 变量浏览器，都按照 MIB 变量的树形命名结构进行设计，这样就可以自顶向下，根据所要浏览的 MIB 变量的类别逐步找到该变量，而无须记住该变量复杂的名字。网络管理人员可以利用 MIB 变量浏览器取出路由器当前的配置信息、性能参数以及统计数据等，对网络情况进行监控。

Microsoft 提供了一个实用程序 Snmputil，可以用于测试 SNMP 服务，也可以用于测试用户开发的扩展代理。

Snmputil 的用法是：

```
Snmputil [get|getnext|walk] agentaddress community old[old…]
Snmputil trap
```

可以使用 Snmputil 发送 GetRequest 或 GetNextRequest 报文，也可以用 Snmputil 遍历整个 MIB 子树。一种较好的测试方法是同时打开两个 DOS 窗口，在一个窗口中用 Snmputil 发送请求，在另一个窗口中用 Snmputil 接收异常报告情况。

4.1.2 典型例题分析

例 1 某一大型园区网，由若干个路由器构成园区网主干。有两台 Windows 2000 主机无法正常通信，我们怀疑是其中某个路由器工作不正确或配置错误而引起的，网络管理员应用什么命令来找到这个路由器？

分析：该题主要考查考生对 tracert 命令的使用和掌握情况。

在 Windows 2000 中提供了一个跟踪程序命令 tracert 可以跟踪数据包经过的路由。该工

具将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标主机，以决定到达目标主机所经历的路由器。由于要求路径上的每个路由器在转发数据包之前至少将 IP 数据包中的 TTL 递减 1，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息送回源主机。路由跟踪程序先发送 TTL 为 1 的回显数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定数据包经过的路由器。如果检查出到哪个路由器之前都能正常响应，到某一个路由器就不能响应了，这样就很容易知道如果线路出现故障，故障点就可能出在某处。

答案：tracert　<目的主机的 IP 地址或域名>

例 2　为了分析一台安装了 Windows Server 2003 服务器的网络流量，使用查看网络状态信息工具 netstat。如果想每 30 秒统计一下 TCP 连接情况，该使用哪些参数？(写出完整命令)

分析：该题主要考查考生对 netstat 命令使用掌握情况。

netstat 命令可以帮助网络管理员了解网络的整体使用情况。它既可以显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息，也可以统计目前总共有哪些网络连接正在运行。其命令格式为

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中，参数-p protocol 用于显示指定协议的网络连接，参数-s 用于显示每个协议的统计，参数 interval 设定重新显示所选统计的间隔时间。因此命令为

```
netstat -s -p TCP 30
```

答案：netstat- s - p TCP 30

4.1.3　同步练习

1．命令“ping 210.45.40.1-t-l 512”的含义是什么？

2．命令“tracert-h 10-w 50 210.45.40.1”的含义是什么？

3．为了分析一台安装了 Windows Server 2003 服务器的网络流量，使用查看网络状态信息工具 netstat。如果想每 30 秒显示一下 UDP 连接情况，并进行统计，该使用哪些参数？(写出完整命令)

4．某台安装了 Windows Server 2003 服务器的装有多块网卡，不同网卡接入了不同网络，管理员通过 Windows Server 2003 中的 route 命令增加了路由表，那么我们使用什么命令来查看这个路由表呢？

4.1.4　同步练习参考答案

1．连续向 IP 地址为 210.45.40.1 的主机发送大小为 512 字节的数据包，以检查该主机是否返回这些数据包的响应。

2．查看数据包从本地主机到 IP 地址为 210.45.40.1 的主机所经过的路由，最大跃点数为 10，等待时间为 50ms。

3．netstat -s -p udp 30

4．netstat -r

4.2 网络故障

4.2.1 考点辅导

4.2.1.1 网络故障诊断与排除的基本概念

网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象出发，以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题的根源、排除故障、恢复网络正常运行的软件或者硬件。网络故障通常有以下几种可能。

- 物理层中物理设备相互连接失败或者硬件及线路本身的问题。
- 数据链路层网络设备的接口配置问题。
- 网络层网络协议配置或操作错误。
- 传输层设备性能或通信拥塞的问题。
- 上三层或网络应用程序错误。

网络故障的诊断过程应该沿着 OSI 七层模型从物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类推，设法确定通信失败的故障点，直到系统通信正常为止。

网络诊断可以使用包括局域网或广域网分析仪在内的多种工具：路由器诊断命令、网络管理工具和其他故障诊断工具。一般情况下，查看路由表是解决网络故障时的首选。ICMP 的 ping、trace 命令和 Cisco 的 show 命令、debug 命令是获取故障诊断有用信息的网络工具。通常使用一个或多个命令收集相应的信息，在给定情况下，确定使用什么命令获取所需要的信息。

网络故障往往以某种症状表现出来，对每一个症状使用特定的故障诊断工具和方法都能查找出一个或多个故障原因。

4.2.1.2 网络故障的分类

根据网络故障的性质把网络故障分为物理故障(硬件故障)与逻辑故障(软件故障)，也可以根据网络故障的对象把网络故障分为线路故障、路由器故障和主机故障。

1．按网络故障的性质分类

首先介绍按照网络故障的不同性质而划分的物理故障(硬件故障)与逻辑故障(软件故障)。

1) 物理故障

物理故障指的是设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。

2) 逻辑故障

逻辑故障中最常见的情况就是配置错误，就是指由于网络主机或网络设备的配置原因

而导致的网络异常或故障。配置错误可能是主机、交换机或路由器端口参数设定有误，或路由器路由配置错误以至于路由循环或找不到远端地址，或者是路由掩码设置错误等。比如，同样是网络中的线路故障，该线路没有流量，但又可以 ping 通线路的两端端口，这时就很有可能是路由配置错误了。遇到这种情况，我们通常用“路由跟踪程序”(在不同系统中的路由跟踪命令并不相同，在 Windows 环境下使用 tracert 命令，在 Linux 或 UNIX 下使用 traceroute 命令，在 Cisco 路由器中使用 trace 命令)，它和 ping 命令类似，最大的区别在于路由跟踪程序是把端到端的线路按线路所经过的路由器分成多段，然后以每段返回响应与延迟。如果发现在路由跟踪程序的结果中某一段之后，两个 IP 地址循环出现，这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 数据包在该线路上来回反复传递。这时，只需更改远端路由器端口配置，就能恢复线路正常。

逻辑故障的另一类情况就是一些重要进程或端口关闭，以及系统的负载过高。比如也是线路中断，没有流量，用 ping 发现线路端口不通，检查发现该端口处于 down 的状态，这就说明该端口已经关闭，因此导致故障。这时只需重新启动该端口，就可以恢复线路的连通了。还有一种常见的故障情况是路由器的负载过高，表现为路由器 CPU 温度太高、CPU 利用率太高，以及内存剩余太少等，如果因此影响网络服务质量，最直接也是最好的办法就是更换路由器，当然要换个好点的。

2. 按网络故障发生地址分类

网络故障根据故障的不同对象也可以划分为线路故障、路由器故障和主机故障。

1) 线路故障

线路故障最常见的情况就是线路不通。诊断这种情况首先应检查该线路上流量是否还存在，然后用 ping 检查线路远端的路由器端口能否响应，用 traceroute 检查路由器配置是否正确，找出问题逐个解决。

2) 路由器故障

线路故障中很多情况都涉及路由器，因此也可以把一些线路故障归结为路由器故障。检测路由器故障，需要利用 MIB 变量浏览器，用它收集路由器的路由表、端口流量数据、计费数据、路由器 CPU 的温度、负载以及路由器的内存剩余量等数据。通常情况下，网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。

3) 主机故障

主机故障常见的现象就是主机的配置不当。如主机配置的 IP 地址与其他主机冲突，或 IP 地址根本就不在子网范围内，由此导致主机无法连通。主机的另一常见故障就是安全故障。

4.2.1.3　网络故障的分层诊断技术

1. 物理层及其诊断

物理层是 OSI 分层结构体系中最基础的一层，它建立在通信媒体的基础上，是系统和通信媒体的物理接口，为数据链路实体之间进行透明传输，为建立、保持和拆除计算机和网络之间的物理连接提供服务。物理层的故障主要表现在设备的物理连接方式不恰当；连接电缆不正确。确定路由器端口物理连接是否完好的最佳方法是使用 show interface 命令，检查每个端口的状态，解释屏幕输出信息，查看端口状态、协议建立状态和 EIA 状态。

2. 数据链路层及其诊断

数据链路层的主要任务是使网络层无须了解物理层的特征而获得可靠的传输。数据链路层为通过链路层的数据进行封装和拆封装、差错检测和一定程度的校正，并协调共享介质。查找和排除数据链路层的故障，需要查看路由器的配置。

3. 网络层及其诊断

网络层提供建立、保持和释放网络层连接的手段，包括路由选择、流量控制、传输确认、中断、差错及故障恢复等。排除网络层故障的基本方法是沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由，然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障。

4.2.1.4 局域网常见故障的排除

虽然网络故障原因多种多样，但总的来讲，不外乎就是硬件问题和软件问题，说得再确切一些，这些问题就是网络连接性故障、网络协议故障和网络配置故障。

1. 网络连接性故障

故障发生后，首先应当考虑的是网络连接性问题。连接性的问题通常涉及网卡、跳线、信息插座、网线、Hub、交换机、Modem 等设备和通信介质。其中，任何一个设备的损坏，都会导致网络连接的中断。连接性通常可采用软件和硬件工具进行测试验证。例如，当某一台电脑不能浏览 Web 时，在网络管理员的脑子中产生的第一个想法就是网络连接性的问题。到底是不是呢？可以通过测试进行验证。看得到网上邻居吗？可以收发电子邮件吗？ping 得通网络内的其他电脑吗？只要其中一项回答为“是”，那就可以断定本机到 Hub 或交换机的连接性没有问题。当然，即使都回答“否”，也不就表明连接性肯定有问题，而是可能会有问题，因为如果电脑的网络协议的配置出现了问题也会导致上述现象的发生。另外，看一看网卡和 Hub 或交换机接口上的指示灯是否闪烁及闪烁是否正常也是个不错的主意。

排除了由于电脑网络协议配置不当而导致故障的可能后，就应该查看网卡和 Hub 的指示灯是否正常，测量网线是否畅通。

1) 故障表现

连接性故障通常表现为以下几种情况。

(1) 电脑无法登录到服务器。

(2) 电脑无法通过局域网接入 Internet。

(3) 电脑在【网上邻居】中只能看到自己，而看不到其他电脑，从而无法使用其他电脑上的共享资源和共享打印机。

(4) 电脑无法在网络内实现访问其他电脑上的资源。

(5) 网络中的部分电脑运行速度异常缓慢。

2) 故障原因

以下原因可能导致连接性故障。

(1) 网卡未安装，或未安装正确，或与其他设备有冲突。

(2) 网卡硬件故障。

(3) 网络协议未安装，或设置不正确。

(4) 网线、跳线或信息插座故障。

(5) Hub 或交换机电源未打开，Hub 或交换机硬件故障，Hub 或交换机端口硬件故障。

(6) UPS 电源故障。

3) 故障排除方法

(1) 确认连接性故障。当出现一种网络应用故障，如无法接入 Internet 时，首先尝试使用其他网络应用，如查找网络中的其他电脑，或使用局域网中的 Web 浏览等。如果其他网络应用可正常使用，如虽然无法接入 Internet，却能够在“网上邻居”中找到其他电脑，则可 ping 通其他电脑，即可排除连接性故障原因。如果其他网络应用均无法实现，则继续下面的操作。

(2) 看 LED 灯判断网卡的故障。首先查看网卡的指示灯是否正常。正常情况下，在不传送数据时，网卡的指示灯闪烁较慢，传送数据时，闪烁较快。如果是不亮，或者是长亮不灭，都表明有故障存在。如果网卡的指示灯不正常，需关掉电脑更换网卡。对于 Hub 或交换机的指示灯，凡是插有网线的端口，指示灯都亮。Hub 指示灯的作用只能指示该端口是否连接有终端设备，而不能显示通信状态。有的交换机指示灯则通过不同的颜色来表示不同的通信状态，例如，用绿色表示正常通信，用橙色表示阻断通信。

(3) 用 ping 命令排除网卡故障。使用 ping 命令，ping 本地的 IP 地址或主机名(如 server01)，检查网卡和 IP 网络协议是否安装完好。如果能 ping 通，说明该电脑的网卡和网络协议设置都没有问题，问题出在电脑与网络的连接上。因此，应当检查网线和 Hub(或交换机)的接口状态，如果无法 ping 通，只能说明 TCP/IP 协议有问题。这时可以在电脑的【控制面板】的【系统】中，查看网卡是否已经安装或是否出错。如果在系统中的硬件列表中没有发现网络适配器，或网络适配器前方有一个黄色的“！”，说明网卡未安装正确，需将未知设备或带有黄色“！”的网络适配器删除。刷新后，重新安装网卡，并为该网卡正确安装配置网络协议，然后进行应用测试。如果网卡无法正确安装，说明网卡可能损坏，必须换一块网卡重试。如果网卡安装正确，则故障原因是协议未安装。

(4) 如果确定在网卡和协议都正确的情况下，网络还是不通，可以初步断定是 Hub(或交换机)和双绞线的问题。为了进一步进行确认，可再换一台主机用同样的方法进行判断。如果其他电脑与本机连接正常，则故障一定在先前那台主机和 Hub(或交换机)的接口上。

(5) 如果确定 Hub(或交换机)有故障，应首先检查 Hub(或交换机)的指示灯是否正常，如果先前那台电脑与 Hub(或交换机)连接的接口灯不亮，说明该 Hub(或交换机)的接口有故障。

(6) 如果 Hub(或交换机)没有问题，则检查电脑到 Hub 的那一段双绞线和所安装的网卡是否有故障。判断双绞线是否有问题可以通过双绞线测试仪或用两块三用表分别由两个人在双绞线的两端测试。主要测试双绞线的 1、2 和 3、6 四条线(其中 1、2 线用于发送，3、6 线用于接收)。如果发现有一根不通就要重新制作。

通过上面的操作，我们就可以判断故障是否出在网卡、双绞线或 Hub(或交换机)上，从而一一予以排除。

2. 网络协议故障

没有网络协议，网络设备和电脑之间就无法实现通信，不能实现资源共享。

1) 协议故障的表现

协议故障通常表现为以下几种情况。

(1) 电脑无法登录到服务器。

(2) 电脑在【网上邻居】中既看不到自己，也无法在网络中访问其他电脑。

(3) 电脑在【网上邻居】中能看到自己和其他成员，但无法访问其他电脑。

(4) 电脑无法通过局域网接入 Internet。

2) 故障原因分析

(1) 协议未安装：实现局域网通信，需安装 NetBEUI 协议，这有助于提高网络速度。

(2) 协议配置不正确：TCP/IP 协议涉及的基本参数有四个，包括 IP 地址、子网掩码、DNS、网关，任何一个设置错误，都会导致故障发生。

3) 排除步骤

当电脑出现以上协议故障现象时，应当按照以下步骤进行故障的定位。

(1) 检查电脑是否安装 TCP/IP 和 NetBEUI 协议，如果没有，建议安装这两个协议，并把 TCP/IP 参数配置好，然后重新启动电脑。

(2) 使用 ping 命令，测试与其他电脑的连接情况。

(3) 在【控制面板】的【网络】属性中，单击【文件及打印共享】按钮，在打开的【文件及打印共享】对话框中检查一下，看看是否选中了【允许其他用户访问我的文件】和【允许其他电脑使用我的打印机】复选框，或者选中了其中的一个。如果都没有选中，则应全部选中或选中其中一个，否则将无法使用共享文件夹。

(4) 系统重新启动后，双击【网上邻居】图标，将显示网络中的其他电脑和共享资源。如果仍看不到其他电脑，可以使用【查找】命令，找到其他电脑。

(5) 在【网络】属性的【标识】中重新为该电脑命名，使其在网络中具有惟一性。

3. 网络配置故障

配置错误也是导致故障发生的重要原因之一。服务器、工作站、交换机、路由器都有自己的配置选项，如果网络管理员对服务器、交换机、路由器等有不当设置就会导致网络故障。例如，对服务器权限的设置不当，会导致资源无法共享的故障。电脑的使用者对电脑设置的修改，也往往会产生一些令人意想不到的访问错误，例如，网卡配置不当，会导致无法连接的故障。

1) 故障表现及分析

配置故障更多地表现在不能实现网络所提供的各种服务上，如不能访问某一台电脑等。因此，在修改配置前，必须做好原有配置的记录，并且最好进行备份。

配置故障通常表现为以下两种。

(1) 电脑只能与某些电脑而不是全部电脑进行通信。

(2) 电脑无法访问任何其他设备。

2)　配置故障排除步骤

首先检查发生故障电脑的相关配置。如果发现错误，修改后，再测试相应的网络服务能否实现。如果没有发现错误，或相应的网络服务不能实现，可执行下述步骤。

测试系统内的其他电脑是否有类似的故障，如果有同样的故障，说明问题出在网络设备上，如 Hub 或交换机。反之，检查被访问电脑对该电脑所提供的服务。

网络故障虽然多种多样，但并非无规律可循。随着理论知识和经验技术的积累，故障排除将变得越来越快，越来越简单。严格的网络管理，是减少网络故障的重要手段；完善的技术档案，是排除故障的重要参考；有效的测试和监控工具，则是预防、排除故障的有力助手。

4.2.2　典型例题分析

例 1　阅读以下说明，回答问题 1～问题 5，将解答填入答题纸对应的解答栏内。(2009 年 11 月下午试题三)

【说明】

某单位通过路由器实现 NAT 转换，网络拓扑结构如图 4-1 所示。其中所有服务器和客户机都使用私网地址，FTP 服务器可对外提供服务。

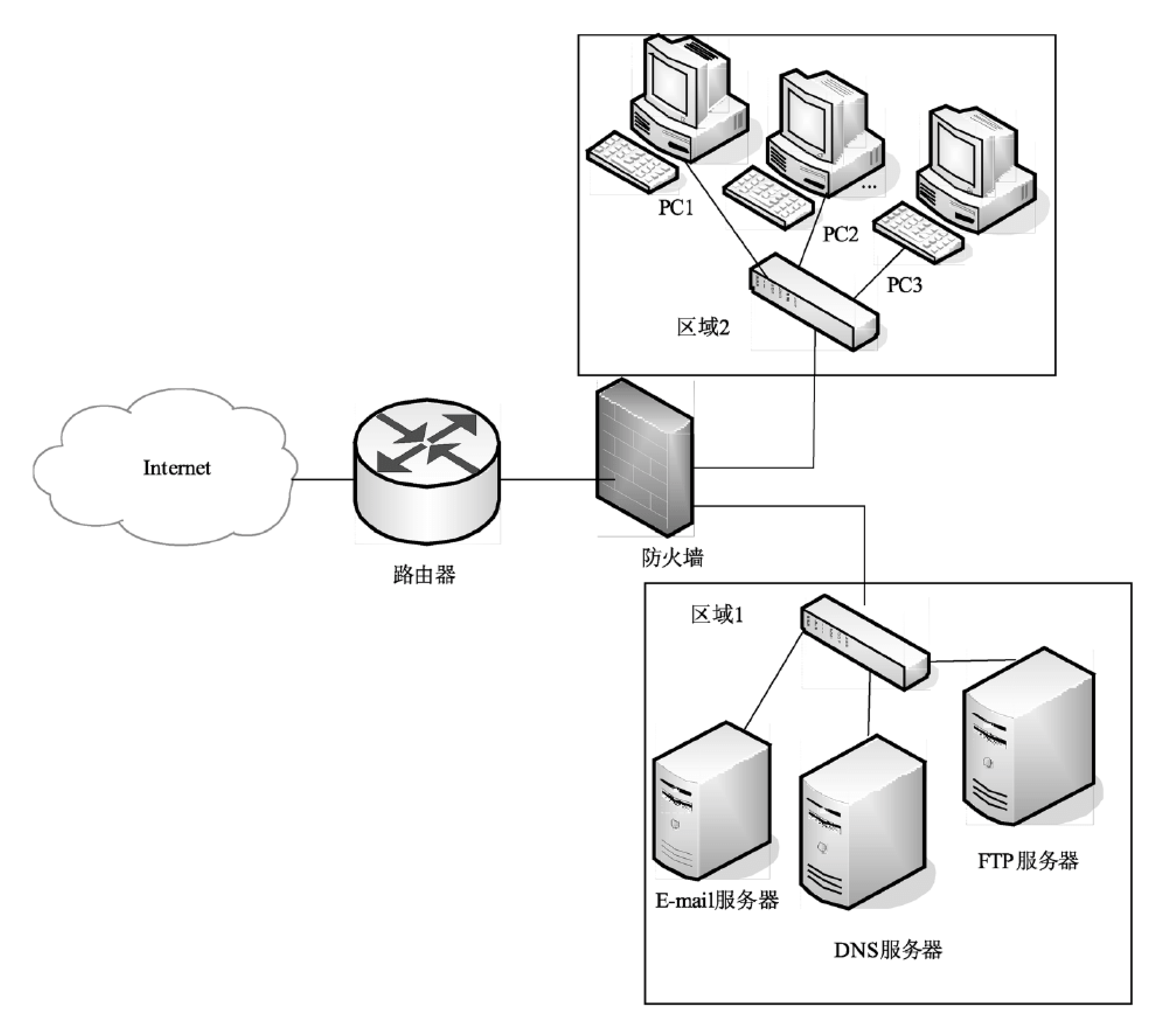


图 4-1　某单位网络拓扑结构

路由器 NAT 映射地址及对应域名如表 4-1 所示。

表 4-1　NAT 映射地址及对应域名表

服务器名称	内网地址	外网映射地址	域　名
FTP 服务器	192.168.1.2	61.11.52.99	ftp.test.com
DNS 服务器	192.168.1.3	61.11.52.100	

【问题 1】(4 分)

该网络中，区域 1 是防火墙的__(1)__。为使该企业网能够接入 Internet，路由器接口 1 可以使用的 IP 地址是__(2)__。

(1) A．DMZ　B．Trust 区域　C．Untrust 区域

(2) A．10.1.1 .1　B．61.11.52.101

C．172.30.1.1　D．192.168.1.1

【问题 2】(4 分)

若需要架设一台 Web 服务器对外提供服务，域名为 www.test.com，外网 IP 地址为 61.11.52.98，内网 IP 地址为 192.168.1.4，则 Web 服务器应该放置在__(3)__。若内网用户可以通过域名正常访问该 Web 服务器，而外网用户无法访问该服务器。经检查，Web 服务器的 DNS 记录配置正确，则可能的原因是__(4)__。

(3) A．区域 1　B．区域 2

(4) A．路由器上 NAT 表项配置错误

B．DHCP 服务器配置错误

C．Web 服务器未启动

【问题 3】(3 分)

若区域 2 中的计算机接入 Internet 时，网络连接时断时续，网络管理员利用 Sniffer 抓包工具分析区域 2 中的分组，发现大量 ARP 应答数据包占用了网络带宽，则可能的故障原因是__(5)__。为了排除故障，网络管理员应采取的措施为__(6)__。

(5) A．网络线路出现故障　B．网络中出现了 ARP 病毒

C．DNS 服务器配置错误　D．防火墙配置错误

【问题 4】(2 分)

某 Windows 客户端开机后无法上网，其他计算机均能正常上网。经过检查，该机网络协议相关配置均正确。使用 ping 命令测试 127.0.0.1 及 FTP 服务器连接，结果如图 4-2 和图 4-3 所示，则可能的故障原因是__(7)__。

A．Web 服务器未启动　B．DNS 服务器未启动

C．客户端机器网络线路故障　D．客户端机器网卡故障

【问题 5】 (2 分)

若某客户机使用 IE 可以正常访问网站，而 QQ 软件不能连网，可能的原因是__(8)__。

A．DNS 服务器配置错误　B．QQ 软件代理配置错误

C．客户端机器网络线路故障　D．客户端机器网卡故障

```
C:\Documents and Settings\Frank>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 4-2　ping 命令测试结果(1)

```
C:\Documents and Settings\Frank>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 4-3　ping 命令测试结果(2)

分析：

【问题 1】

DMZ(非军事化区域)，是一个小型网络，存在于公司的内部网络和外部网络之间。DMZ 用来作为一个额外的缓冲区以进一步隔离公网和内部私有网络。Trust 区域，简单说就是一个内网(trust)，是安全可信任的区域。Untrust 区域，是不安全不可信的区域。故(1)题选 A。由表 4-1 可知，FTP 服务器和 DNS 服务器的外网映射地址分别为 61.11.52.99、61.11.52.100，可以排除 A、C、D，故(2)题选 B。

【问题 2】

由题意和 DMZ 的概念可知，Web 服务器应该放在 DMZ 内，故(3)题选 A。由题意可知，内网用户可以通过域名正常访问该 Web 服务器，说明 Web 服务器是启动了的，DHCP 服务器配置是正确的，故(4)选 A。NAT 指网络地址转换，是通过数据包的源地址或者目的地址来达到节省 IP 地址资源，隐藏内部 IP 地址功能的一种技术。

【问题 3】

ARP 病毒指 ARP 木马攻击，病毒会将该机器的 MAC 地址映射到网关的 IP 地址上，向局域网内大量发送 ARP 包，致同一网段地址内的其他机器误将其作为网关，掉线时，内网是互通的，计算机却不能上网。故(5)题选 B。采取的措施一般为查找出感染 ARP 病毒的计算机，使用专用工具查杀病毒。

【问题 4】

Ping 命令的返回结果代表的含义如下。

①　“Request timed out.”表示没有收到目标主机返回的响应数据包，也就是网络不通或网络状态恶劣。

②　“Reply from X.X.X.X: bytes=32 time<1ms TTL=128”表示收到从目标主机 X.X.X.X 返回的响应数据包，数据包大小为 32B，响应时间小于 1ms TTL 为 128，这个结果表示您的计算机到目标主机之间连接正常。

③　“Destination host unreachable”表示目标主机无法到达。

④ “PING: transmit failed,error code XXXXX”表示传输失败。通过错误代码 XXXXX 可知它的命令格式和使用方法，然后我们就可以开始检查到底是哪个地方出问题了。

ping 127.0.0.1，127.0.0.1 这个 IP 地址被定义为本机 IP 地址，如果返回的是第二种结果，则表示网卡驱动及 TCP/IP 都是正常的。如果返回的是第四种结果则表示网卡驱动程序或 TCP/IP 有问题，此时应该检查一下网卡驱动程序是否安装正确，TCP/IP 协议是否安装。由图 3-2 可知，网卡驱动及 TCP/IP 都是正常的。

ping 局域网内其他的 IP，如果收到 0 个应答，表示电缆系统有问题。图 4-2 可知，显示无法到达目的主机，则可能是客户端机器网络线路故障，故(7)题选 C。

【问题 5】

由于 IE 能正常访问网站，故 DNS 服务器配置、客户端机器网络线路以及客户端机器网卡都是正常工作的，否则 IE 无法上网，故(8)题选 B。当 QQ 软件代理配置错误时，QQ 软件是无法连网的。

答案：

【问题 1】

(1) A

(2) B

【问题 2】

(3) A

(4) A

【问题 3】

(5) B

(6) 查找出感染 ARP 病毒的计算机，使用专用工具查杀病毒

【问题 4】

(7) C

【问题 5】

(8) B

例 2 阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 11 月下午试题一)

【说明】

某公司采用代理服务器接入 Internet，网络拓扑结构如图 4-4 所示。

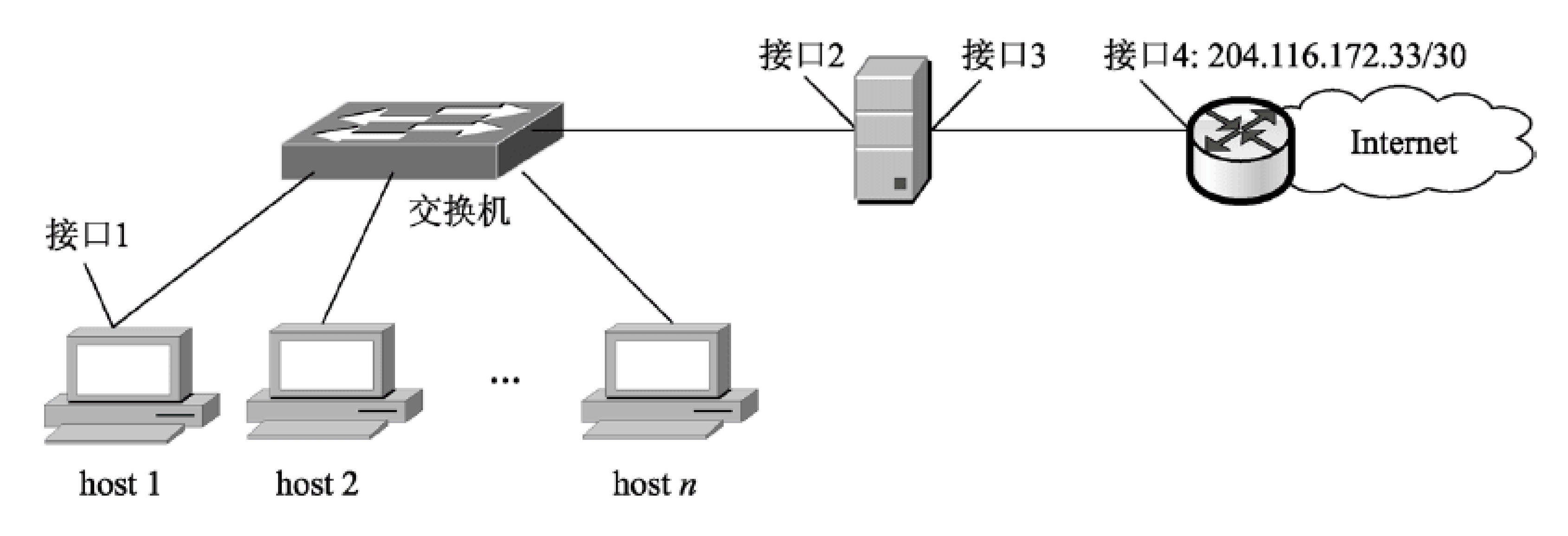


图 4-4 代理服务器功能示意图

在 host 1 的 DOS 命令窗口中，运行 route print 命令显示其路由信息，得到的结果如图 4-5 所示。

```
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  118.165.3.190  118.165.3.178     20
    118.165.3.128  255.255.255.192  118.165.3.178  118.165.3.178     20
    118.165.3.178  255.255.255.255      127.0.0.1      127.0.0.1     20
  118.255.255.255  255.255.255.255  118.165.3.178  118.165.3.178     20
        127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1      1
        224.0.0.0        240.0.0.0  118.165.3.178  118.165.3.178     20
  255.255.255.255  255.255.255.255  118.165.3.178  118.165.3.178      1
```

图 4-5　route print 命令运行结果

【问题 1】(8 分)

请填写 host 1 的 Internet 协议属性参数。

IP 地址：　　　　__(1)__

子网掩码：　　　　__(2)__

默认网关：　　　　__(3)__

其中，host 1 默认网关为图中接口__(4)__处的 IP 地址。

【问题 2】(3 分)

若 host 1 要访问 Internet，根据默认路由，数据报文经 IP 地址为__(5)__的接口发送到 IP 地址为__(6)__的网关。

【问题 3】(2 分)

与命令 route print 作用等价的命令为__(7)__。

A．netstat -r　　B．ping　　C．tracert　　D．arp –a

【问题 4】(2 分)

接口 3 的 IP 地址为__(8)__。

分析：

路由表中每一个路由表项(或路由)都由五个字段组成。

① 网络目标地址(Network Destination)：代表某个可能的目的地址。它是一个 IP 地址或子网，即表示 IP 数据包被转发到何处的地址。

② 掩码(Netmask):一个用于将某数据包中的 IP 地址中的目标地址字段与上面可能的网络地址匹配起来的位模式。

③ 网关(Gateway)：下一跳的 IP 地址。数据包必须被转发到此，才能到达特定的目的网络。

④ 接口(Interface)：下一跳的接口。这个接口必须用于将数据包进行转发，以达到特定的目的网络。

⑤ 跳数(metric)：表示到达目的的过程中经过了多少跳数(路由器数)，即路由的成本。

【问题 1】

第一行表示发向任意网段的数据通过本机接口 118.165.3.178 被送往一个默认的网关 118.165.3.190，它的代价是 20。故(1)、(3)和(4)的答案分别为 118.165.3.178、118.165.3.190

和 2，第二行中的目的网络与本机处于同一个局域网，可知子网掩码为 255.255.255.192，从而可得到(2)题的答案。

【问题 2】

由上一个问题的分析可知，若 host 1 要访问 Internet，根据默认路由可知，数据报文经 IP 地址为 118.165.3.178 的接口发送到 IP 地址为 118.165.3.190 的网关。可得出(5)和(6)的答案。

【问题 3】

netstat 命令是一个观察网络连接状态的实用工具。它能检验 IP 的当前连接状态，在断定你的基本级通信正在进行后，就要验证系统上的服务。netstat -r 命令的功能为显示路由表，功能与 route print 等价。故(7)选 A。

【问题 4】

由路由器接口 4 的 IP 地址可知，接口 3 的地址应该选择 204.116.172.34。

答案：

【问题 1】

(1) 118.165.3.178

(2) 255.255.255.192

(3) 118.165.3.190

(4) 2

【问题 2】

(5) 118.165.3.178

(6) 118.165.3.190

【问题 3】

(7) A

【问题 4】

(8) 204.116.172.34

例 3 阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 5 月下午试题一)

【说明】

某公司拥有一个 C 类地址块 212.253.115.0/24，网络拓扑结构如图 4-6 所示。

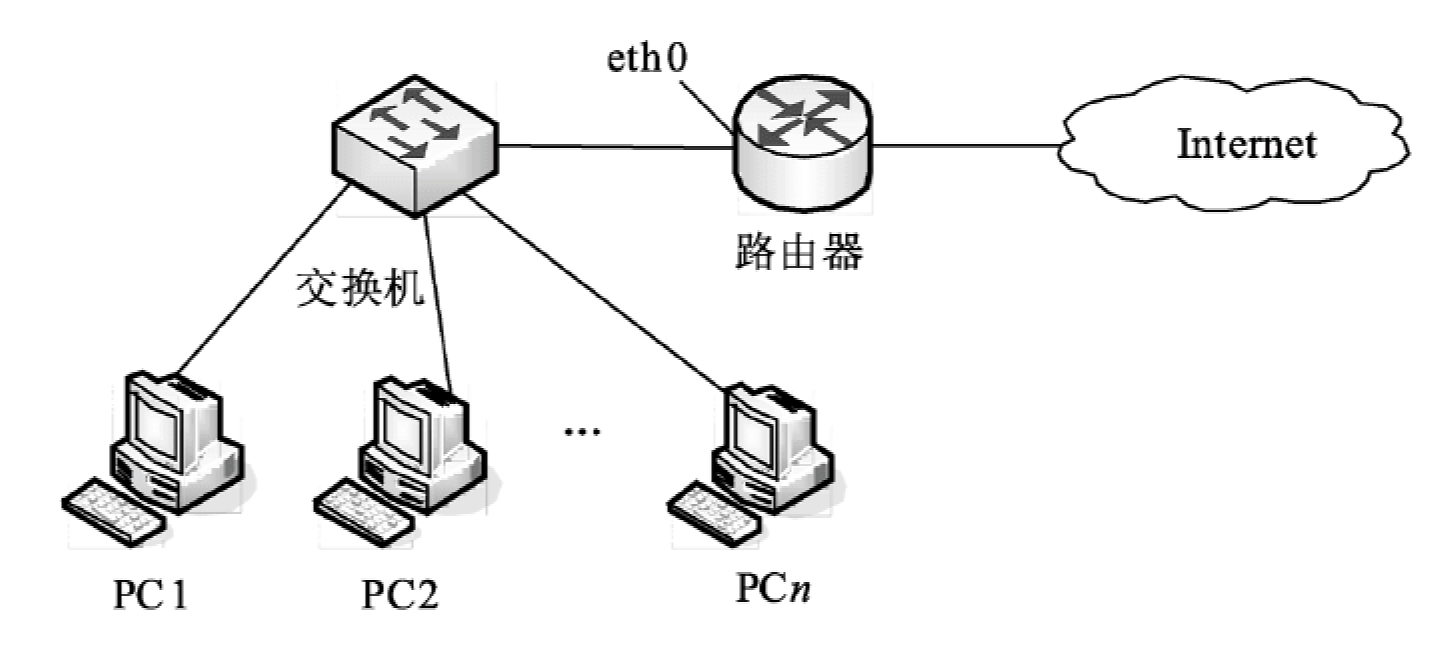


图 4-6 某公司网络拓扑结构

在 PC1 的 DOS 命令窗口中，运行 arp-a 命令显示 PC1 的 ARP 缓存，得到的结果如图 4-7 所示。

```
C:\Documents and SettingsUSER>arp -a

Interface 212.253.115.31---0x3

 Internet Address     Physical Address      Type

 212.253.115.7        0a-1e-0c-83-94-b6     dynamic

 212.253.115.13       0b-23-d3-08-86-98     dynamic

 212.253.112.221      0c-3f-ea-f7-ed-72     dynamic

 212.253.115.254      0d-4f-35-23-5d-8a     dynamic
```

图 4-7　运行 arp-a 命令结果

采用抓包工具在 PC1 中捕获的、由 PC1 以太网接口发出的某数据包的部分信息如图 4-8 所示。

```
以太帧：
    目的地址：  0d:4f:35:23:5d:8a
    源地址：  10:0e:3c:95:64:e5
IP 分组：
    源地址：212.253.115.31
    目的地址：202.205.3.144
TCP 段：
    源端口：1266
    目的端口：80
```

图 4-8　数据包部分信息

【问题 1】(7 分)

请填写图 4-6 中 PC1 的相应参数。

IP 地址：　　　　　　　　　(1)　(1 分)

子网掩码：　　　　　　　　(2)　(2 分)

默认网关：　　　　　　　　(3)　(2 分)

以太网接口的 MAC 地址：　(4)　(2 分)

【问题 2】(4 分)

请填写图 4-6 中路由器 eth0 网卡的相应参数。

IP 地址：　(5)

MAC 地址：__(6)__

【问题 3】(2 分)

在图 4-7 中若要删除某条 ARP 记录，可以采用__(7)__命令。

A. arp -s　　B. arp -d　　C. arp -c　　D. arp -a

【问题 4】(2 分)

图 4-8 表明，在默认情况下该数据包请求的服务为__(8)__。

分析：

【问题 1】由 PC1 以太网接口发出的某数据包 IP 分组的源地址为 212.253.115.31，源地址为主机 IP 地址。该 IP 地址为 C 类地址，可知子网掩码为 255.255.255.0。以太帧中源地址 10:0e:3c:95:64:e5 便是以太网接口的 MAC 地址。以太帧中目的 MAC 地址 0d:4f:35:23:5d:8a 为下一跳路由器的 MAC 地址，即所在局域网与路由器相连端口的 MAC 地址。该 MAC 地址对应的 IP 地址为 212.253.115.254，可知默认网关为 212.253.115.254。

【问题 2】由问题 1 的分析可知，路由器 eth0 网卡的 IP 地址为 212.253.115.254，MAC 地址为 0d-4f-35-23-5d-8a。

【问题 3】arp –s 命令用于添加一个 ARP 记录。arp -d 用于删除指定的 ARP 记录。arp –a 命令用于显示当前的 ARP 记录。

【问题 4】由图 4-8 可知，目的端口为 80，超文本传输协议 HTTP 使用 TCP 协议，默认端口号为 80。HTTP 协议用于在 Web 浏览器和 Web 服务器之间传输页面等内容，提供 Web 服务。

答案：

【问题 1】(1) 212.253.115.31　　(2) 255.255.255.0

(3) 212.253.115.254　　(4) 10:0e:3c:95:64:e5

【问题 2】(5) 212.253.115.254　　(6) 0d-4f-35-23-5d-8a

【问题 3】B

【问题 4】Web 服务或 WWW 服务

例 4　阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 5 月下午试题三)

【说明】

某单位网络拓扑结构如图 4-9 所示。内部服务器和客户机使用私网地址，由路由器实现 NAT 转换。该单位在互联网上注册了域名 test.com，在完成了网络和服务器的部署后，测试服务器与客户端均可正常访问 Internet。

该单位服务器 NAT 映射地址及对应域名如表 4-2 所示。

【问题 1】(空(1)1 分，空(2)2 分，共 3 分)

Web 服务器和邮件服务器由本单位的 DNS 服务器解析，在使用中发现外网无法解析服务器 IP 地址。网络管理员在管理机 PC1 上使用 nsloopup，得到如图 4-10 所示的结果。

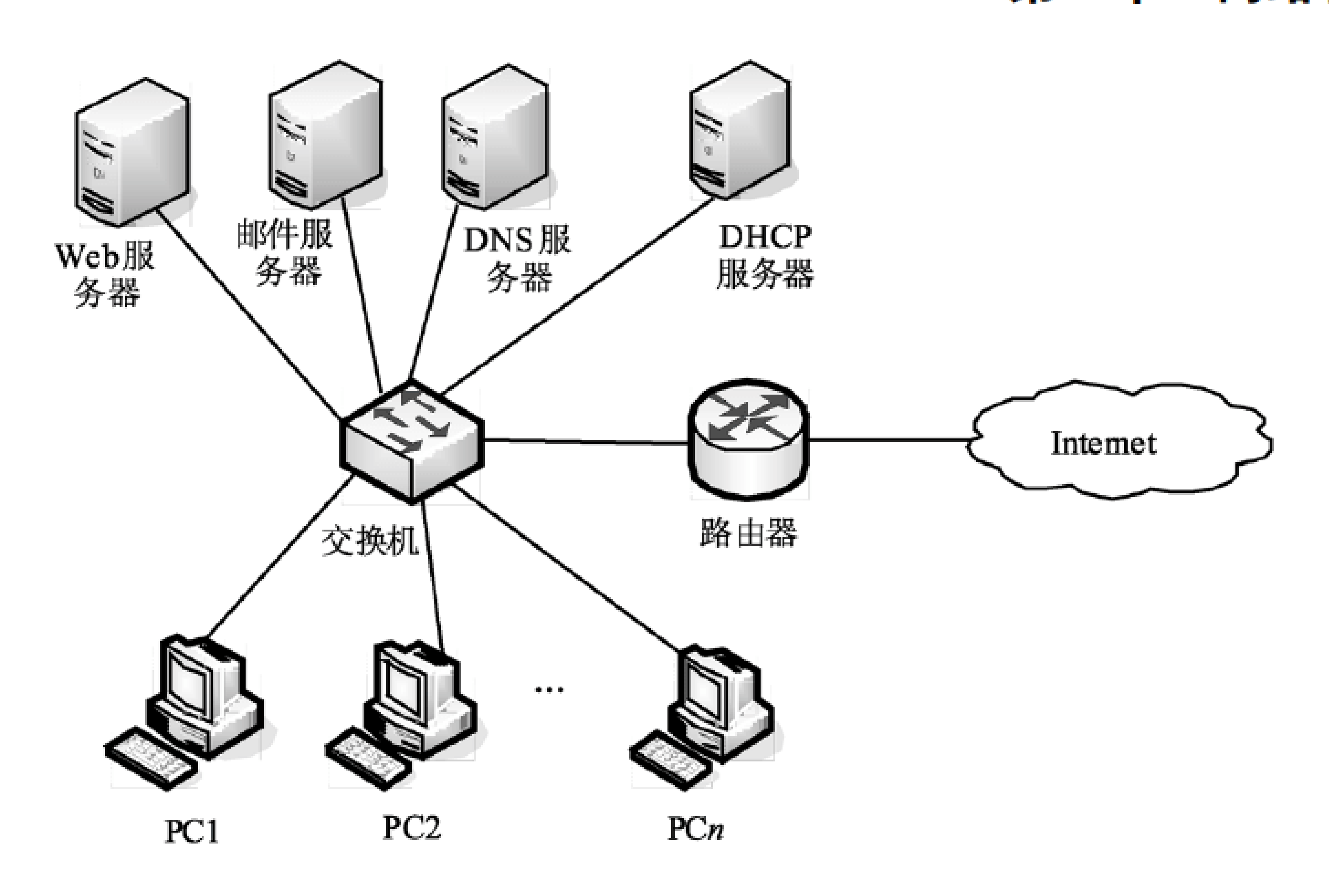


图 4-9　某单位网络拓扑结构

表 4-2　NAT 映射地址及对应域名

服务器名称	内网地址	外网映射地址	域　名
Web 服务器	192.168.1.1	53.21.22.98	www.test.com
邮件服务器	192.168.1.2	53.21.22.99	mail.test.com
DNS 服务器	192.168.1.3	53.21.22.100	

```
C:\Documents and Settings\Administrator>nslookup
Default Server:    nsl.acc.com
Address: 61.32.35.17
> set type=ns
> test.com
Server: nsl.acc.com
Address: 61.32.35.17
Non-authoritative answer
test.com    nameserver = nsl.test.com
nsl.test.com    internet address = 192.168.1.3
```

图 4-10　运行 nsloopup 命令的结果

由以上结果可知：

① PC1 上的首选 DNS 服务器的 IP 地址为__(1)__。

A. 53.21.22.100　　B. 61.32.35.17　　C. 192.168.1.3　　D. 192.168.1.1

② DNS 服务器无法对外解析 IP 地址的原因是__(2)__。

A. DNS 服务器设置中名称服务器地址使用了内网地址

B. DNS 服务器中未设置名称服务器

C. DNS 服务器未启动

D. Web 服务器工作异常

【问题 2】(6 分)

网络管理员调整 DNS 服务器配置后，Web 服务器工作正常，邮件服务器只能对外发送邮件，但不能接收外部邮件，网络管理员测试发现邮件服务器本身工作正常。

① 网络管理员在外网使用以下命令测试邮件服务器域名解析是否正常，请完成该命令。

ping ___(3)___

② 网络管理员在外网使用以下命令测试连接邮件服务器邮件接收端口是否正常，正确的测试命令是：___(4)___。

A. telnet mail.test.com :110　　B. telnet mail.test.com 110

C. telnet mail.test.com:25　　D. telnet mail.test.com25

③ 如果以上测试没有发现问题，则故障是由于___(5)___。

A. 邮件服务器未启动　　B. 邮件服务器连通故障

C. DNS 服务器未设置 mail 主机地址映射　　D. DNS 服务器未设置 mx 记录

【问题 3】(4 分)

该单位网络中，客户端全部从 DHCP 服务器处动态获取 IP 地址，该 DHCP 服务器设置的地址池为 192.168.1.1～192.168.1.253。

① 该单位服务器发现与其他计算机 IP 地址冲突，网络管理员检查发现本网络内设有其他 DHCP 服务器，并且除服务器外其他客户端没有设置静态 IP 地址。此时应检查调整 DHCP 服务器的___(6)___。

② 某 Windows 客户端开机后发现无法上网，使用 ipconfig 发现本机自动获取的 IP 地址是 169.254.8.1，此时检查 DHCP 服务器工作正常，且地址池中尚有未分配地址。此时应检查___(7)___。

【问题 4】(2 分)

某客户端发现访问外网正常，只是在访问 http://www.abc.com 网站时，总是访问到本单位的 Web 服务器，而同一网段内的其他客户端访问该网站时是正常的，该客户端与其他客户端都是通过 DHCP 服务器获取同一作用域的 IP 地址和 DNS 服务器地址，此时应检查本机的___(8)___文件。

A. 注册表　　B. hosts　　C. config　　D. autoexec

分析：

【问题 1】nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令工具。当用户设置好域名服务器之后，就可以用这个命令查看不同主机的 IP 地址对应的域名。在命令行提示符中输入 nslookup 命令后，显示的 DNS 服务器域名为 nsl.acc.com，其 IP 地址为 61.32.35.17，可见 PC1 上的首选 DNS 服务器的 IP 地址为 61.32.35.17。

名字服务器(Name Server)用 NS 标明域的名字服务器，可以通过“set type=NS”命令查询与根域相关的所有 NS 类型记录。查询结果中出现“Non-authoritative answer:”，这表明没有到网络外去查询，而是在缓存区中查找并找到数据。通过图 4-10 的最后一行可知，名字服务器的地址为 192.168.1.3，这是一个内网地址。可见是由于 DNS 服务器设置中名称服务器地址使用了内网地址而导致无法对外解析 IP 地址。

【问题 2】成功接收来自 Internet 的邮件需要做到以下三点。

① 要拥有 Internet 上的有效域名。使用 ping domain-name 命令可验证对应服务器是否已经启动。如果出现故障，则表示 DNS 服务器无法对域名正常解析或 DNS 服务器有故障。要测试邮件服务器域名解析是否正常，可使用 ping mail.test.com 命令。

② 邮件服务器在 110 端口成功启动了 POP3 服务。外网用户向内网发送邮件的过程为：外网客户端使用 STMP 协议将邮件发到邮件服务器，发方邮件服务器使用 STMP 协议将邮件发送到内网的邮件服务器 mail.test.com，内网邮件服务器使用 POP3 协议将接收到的邮件存储在内网用户的邮箱中。如果邮件服务器 mail.test.com 不能接收外部邮件，可检查 POP3 协议默认的 TCP 端口 110 是否正常工作，测试命令是：telnet mail.test.com 110。

③ 将此域名的 MX 记录正确解析到邮件服务器的 IP 地址。邮件服务器中的邮件地址格式为："xxx@test.com"，"test.com" 是一个域名。域名只是一个逻辑组合概念，它并不代表真正的计算机，对于使用域名 test.com 作为后缀的邮件地址，外界发送给它的电子邮件必须由一台专门的 SMTP 服务器来进行接收和处理，接收和处理该域的电子邮件的 SMTP 服务器即为该域的 SMTP 服务器，外界发送给某个域的电子邮件实际上都是发送给该域的 SMTP 服务器。外界如何知道一个域的 SMTP 服务器的地址呢？这是通过管理该域的 DNS 服务器上的 MX 记录来获得的。当外部某台 SMTP 服务器要给 "xxx@ test.com" 发送一封电子邮件时，该 SMTP 服务器将根据邮件地址的后缀部分而去查询 "test.com" 这个域的 MX 记录，得到这个域的 SMTP 服务器的主机名为 "mail.test.com"，然后将邮件发送给 "mail.test.com" 这个 SMTP 服务器。如果 DNS 服务器未设置 mx 记录，则外部 SMTP 服务器无法获得域 test.com 的 SMTP 服务器的地址，也就无法将邮件投递到该服务器。

【问题 3】网络内有多个 DHCP 服务器，那么在创建 DHCP 服务器的 IP 作用域时，应排除手工分配给其他服务器、非 DHCP 客户端等的 IP 地址，否则会出现 IP 地址冲突问题。例如，DHCP 服务器 A 作用域的地址范围包括地址 I，DHCP 服务器 B 作用域的地址范围也包括地址 I，如果 DHCP 服务器 A 将地址 I 分配给计算机 M，而 DHCP 服务器 B 将地址 I 分配给计算机 *n*，此时就会出现 IP 地址冲突。所以 IP 地址冲突时，应检查调整 DHCP 服务器的排除 IP 地址范围。

DHCP 服务器设置的地址池为 192.168.1.1～192.168.1.253，且工作正常，而客户机自动获取的 IP 地址是 169.254.8.1，显然不是通过该 DHCP 服务器分配的 IP 地址。由于客户机无法上网，此时应检查网线连接是否正常。

【问题 4】hosts 文件包含了 IP 地址和主机名的映射。同一网段内的其他客户端访问网站 http://www.abc.com 时是正常的，这说明网站工作是正常的。该客户端在访问 http://www.abc.com 网站时，首先通过 DNS 服务器进行域名解析，得到该网站的 IP 地址。之所以访问到本单位的 Web 服务器，可能是因为域名解析得到的 http://www.abc.com 网站 IP 地址与本单位 Web 服务器的 IP 地址一致，此时可以通过 hosts 文件查看该网站的 IP 地址和主机名之间的映射。

答案：

【问题 1】(1) B　(2) A

【问题 2】(3) mail.test.com　(4) B　(5) D

【问题 3】(6) 排除 IP 地址范围　(7) 网线连接

【问题 4】(8) B

例 5　阅读以下说明，回答问题 1～问题 2，将解答填入答题纸对应的解答栏内。(2006 年 11 月下午试题一)

【说明】

某校园网络拓扑结构如图 4-11 所示。

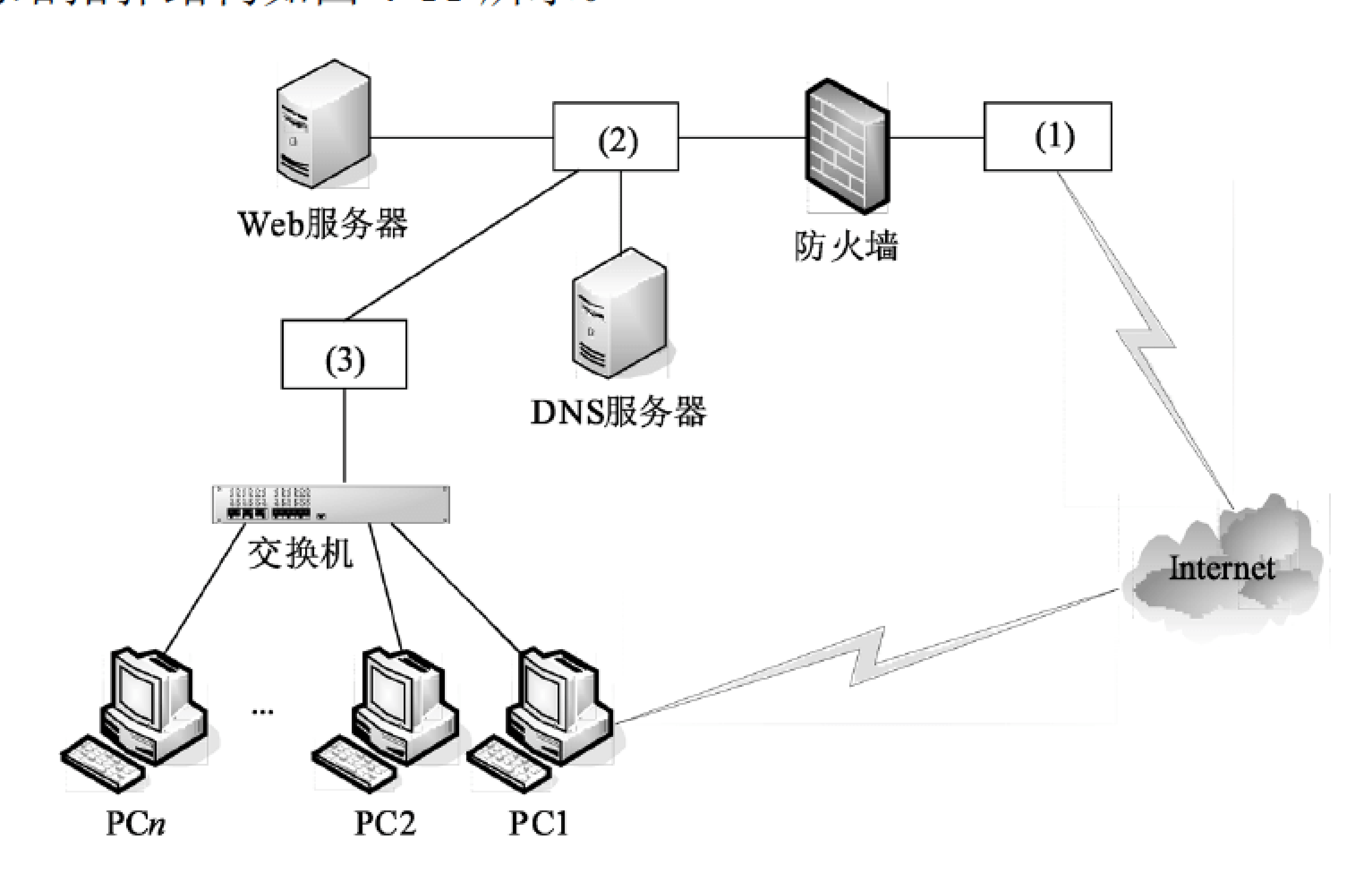


图 4-11　某校园网络拓扑结构

【问题 1】(6 分)

图 4-12 是 PC1 在 Windows 操作系统 cmd 窗口下运行 ipconfig/all 得到的配置信息。

```
Ethernet adapter Local connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : 00-08-74-9B-15-48

PPP adapter Dial-up connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 218.66.0.36
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 218.66.0.36
        DNS Servers . . . . . . . . . . . : 218.85.157.99
                                            202.101.98.55
```

图 4-12　PC1 配置信息

PC1 以太网卡的 MAC 地址为__(1)__；此时采用__(2)__方式接入 Internet，ISP 分配的 IP 地址为__(3)__。

(1)　A. 218.85.157.99　　B. 218.66.0.36
　　C. 00-53-45-00-00-00　　D. 00-08-74-9B-15-48

(2)　A. 局域网　　B. VPN　　C. 拨号连接　　D. 无线上网

(3)　A. 218.85.157.99　　B. 218.66.0.36
　　C. 00-53-45-00-00-00　　D. 00-08-74-9B-15-48

【问题 2】(4 分)

PC*n* 不能访问 Web 服务器，网管员作了如下检查。

① PC*n* 可以通过 Internet 进行 QQ 聊天。

② 外部网络可以访问本地 Web 服务器。

③ 在 Windows Server 2003 作为操作系统的 Web 服务器中运行__(4)__，通过捕获窗口的统计数据，发现网络利用率平均维持在 20%左右。

可能的故障原因是__(5)__。

(4) A. 路由和远程访问　　B. 事件查看器

C. 网络监视器　　D. 远程协助

(5) A. PC*n* 的 IP 地址设置错误　　B. 防火墙阻止 PC*n* 访问 Web 服务器

C. Web 服务器遭受 DoS 攻击　　D. DNS 服务器故障

分析：

【问题 1】

图中 Ethernet adapter Local connection 为以太网适配器的本地连接信息，连接状态为“未连接”，描述为 3Com 3C920，MAC 地址为 00-08-74-9B-15-48。

PPP adapter Dial-up connection 为拨号连接网络信息，其中 ISP 分配的 IP 地址为 218.66.0.36。

因此，(1)～(3)分别应选 D、C、B。

【问题 2】

Microsoft Windows Server 2003 的“路由和远程访问”服务是一个全功能的软件路由器，也是用于路由和互联网络工作的开放平台。它为局域网和广域网环境中的商务活动，或使用安全虚拟专用网连接的 Internet 上的商务活动提供路由选择服务。“路由和远程访问”服务的优点之一是与 Microsoft Windows Server 2003 家族集成。“路由和远程访问”服务提供了很多经济功能，并且和多种硬件平台和数以百计的网卡一起工作。“路由和远程访问”服务可以通过应用程序编程接口(API)进行扩展，开发人员可以使用 API 创建客户网络连接方案，新供应商可以使用 API 参与到不断增长的开放互联网商务中。“路由和远程访问”的服务器是专门为已经熟悉路由协议和路由服务的系统管理员而设计的。通过“路由和远程访问”服务，管理员可以查看和管理其网络上的路由器和远程访问服务器。

事件查看器可以完成许多工作，如审核系统事件和存放系统、安全及应用程序日志等。系统日志中存放了 Windows 操作系统产生的信息、警告或错误。通过查看这些信息、警告或错误，用户不仅可以了解到某项功能配置或运行成功的信息，还可了解到系统的某些功能运行失败或不稳定的原因。安全日志中存放了审核事件是否成功的信息。通过查看这些信息，可以了解到这些安全审核结果为成功还是失败。应用程序日志中存放应用程序产生的信息、警告或错误。通过查看这些信息、警告或错误，可以了解到哪些应用程序成功运行，产生了哪些错误信息或者潜在错误。程序开发人员可以利用这些资源来改善应用程序。

“网络监视器”是从 Windows 2000 Server 就开始引入的一个监视网络通信状况的服务器组件，它可以细致到监视一个数据包的具体内容，以供用户详细了解服务器的数据流动情况。使用“网络监视器”可以帮助网络管理员查看网络故障、检测黑客攻击。

“远程协助”功能虽然自 Windows XP 系统就开始有了，但对于 Windows 2000 Server

来说，仍属于新增内容。用户可以使用“远程协助”来邀请受信任的个人与自己聊天、观察用户的工作屏幕，并在得到用户的许可后远程控制用户的计算机。也可使用“远程协助”来远程管理计算机。

因此，(4)应选 C。

PC*n* 可以通过 Internet 进行 QQ 聊天，可以排除“PC*n* 的 IP 地址设置错误”；外部网络可以访问本地 Web 服务器以及网络利用率平均维持在 20%左右，可以排除“Web 服务器遭受 DoS 攻击”；PC*n* 访问 Web 服务器不需要经过防火墙，排除“防火墙阻止 PC*n* 访问 Web 服务器”。因此，可能的故障原因是 DNS 服务器故障，故(5)应选 D。

答案：

【问题 1】

(1) D (2) C (3) B

【问题 2】

(4) C (5) D

例 6 阅读以下说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2006 年 11 月下午试题二)

【说明】

在 SNMP 服务安装完成后，Windows Server 2003 的服务如图 4-13 所示。

在图 4-14 所示的配置界面中单击【接受团体名称】中的【添加】按钮，在如图 4-15 所示的界面中设置【团体名称】选项；在图 4-14 中单击【接受来自这些主机的 SNMP 数据包(T)】中的【添加】按钮，在如图 4-16 所示的界面中加入 IP 地址。

名称	描述	状态	启动类型	登录为
Server	支...	已启动	自动	本地系统
Shell Hardware ...	为...	已启动	自动	本地系统
Simple Mail Tra...	跨...	已启动	自动	本地系统
Smart Card	管...		手动	本地服务
SNMP Service	使...	已启动	自动	本地系统
SNMP Trap Service	接...	已启动	手动	本地服务
Special Adminis...	允...		手动	本地系统
System Event No...	监...	已启动	自动	本地系统
Task Scheduler	使...	已启动	自动	本地系统
TCP/IP NetBIOS ...	提...	已启动	自动	本地服务
Telephony	提...	已启动	手动	本地系统
Telnet	允...		禁用	本地服务
Terminal Services	允...	已启动	手动	本地系统
Terminal Servic...	允...		禁用	本地系统
Themes	为...		禁用	本地系统
Uninterruptible...	管...		手动	本地服务
Upload Manager	管...		手动	本地系统

图 4-13 【服务】配置界面

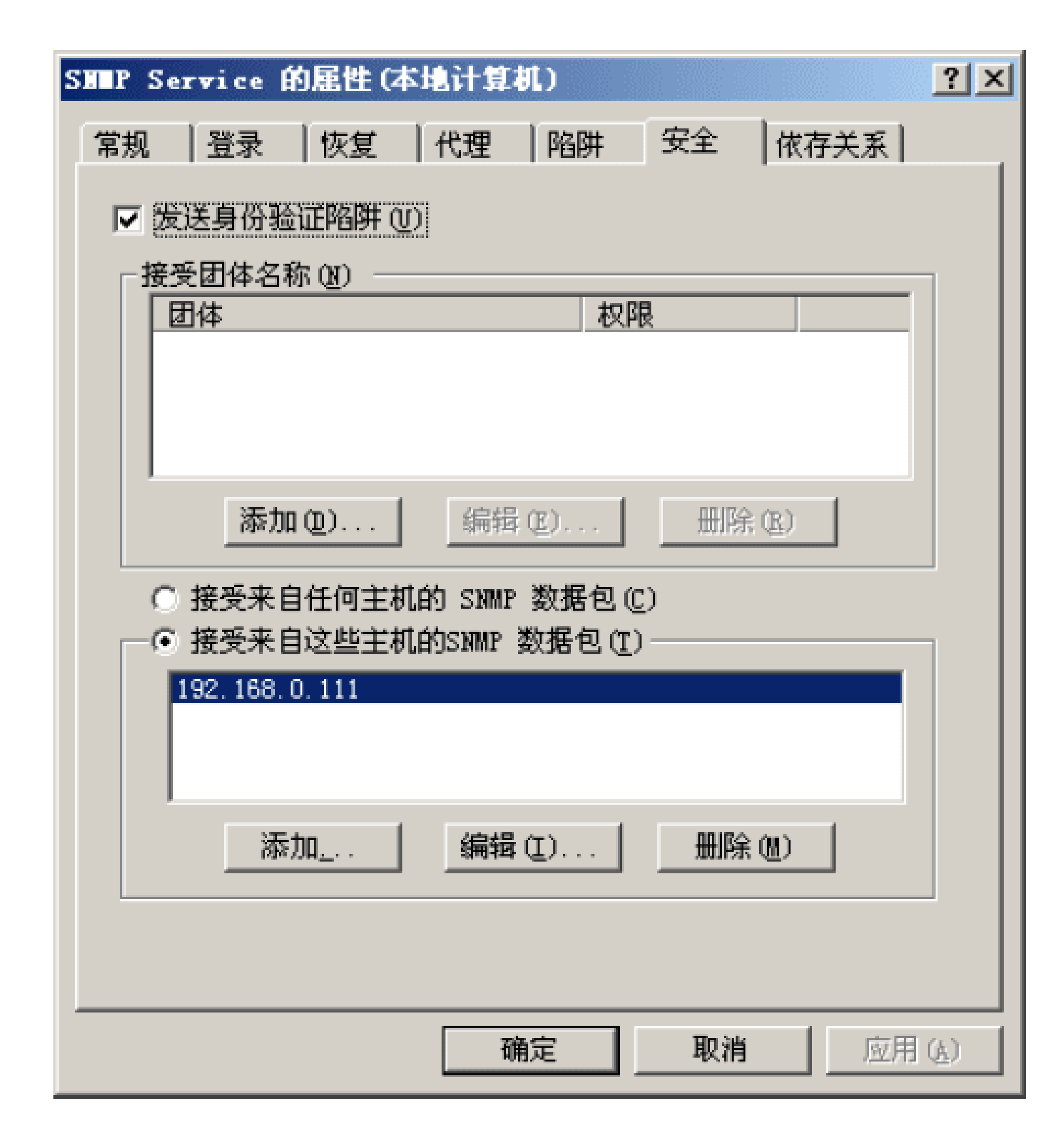


图 4-14 【SNMP Service 的属性】配置界面

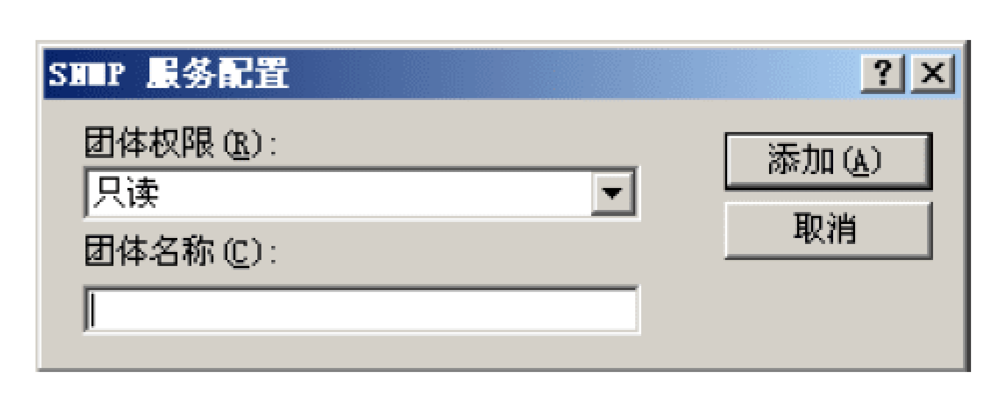


图 4-15 【SNMP 服务配置】对话框(1)



图 4-16 【SNMP 服务配置】对话框(2)

将 snmputil 复制到 IP 地址为 192.168.0.111 的系统中，在 cmd 窗口中输入命令：snmputil walk192.168.0.110public.1.3.6.1.4.1.77.1.2.25.1.1，显示结果如图 4-17 所示。

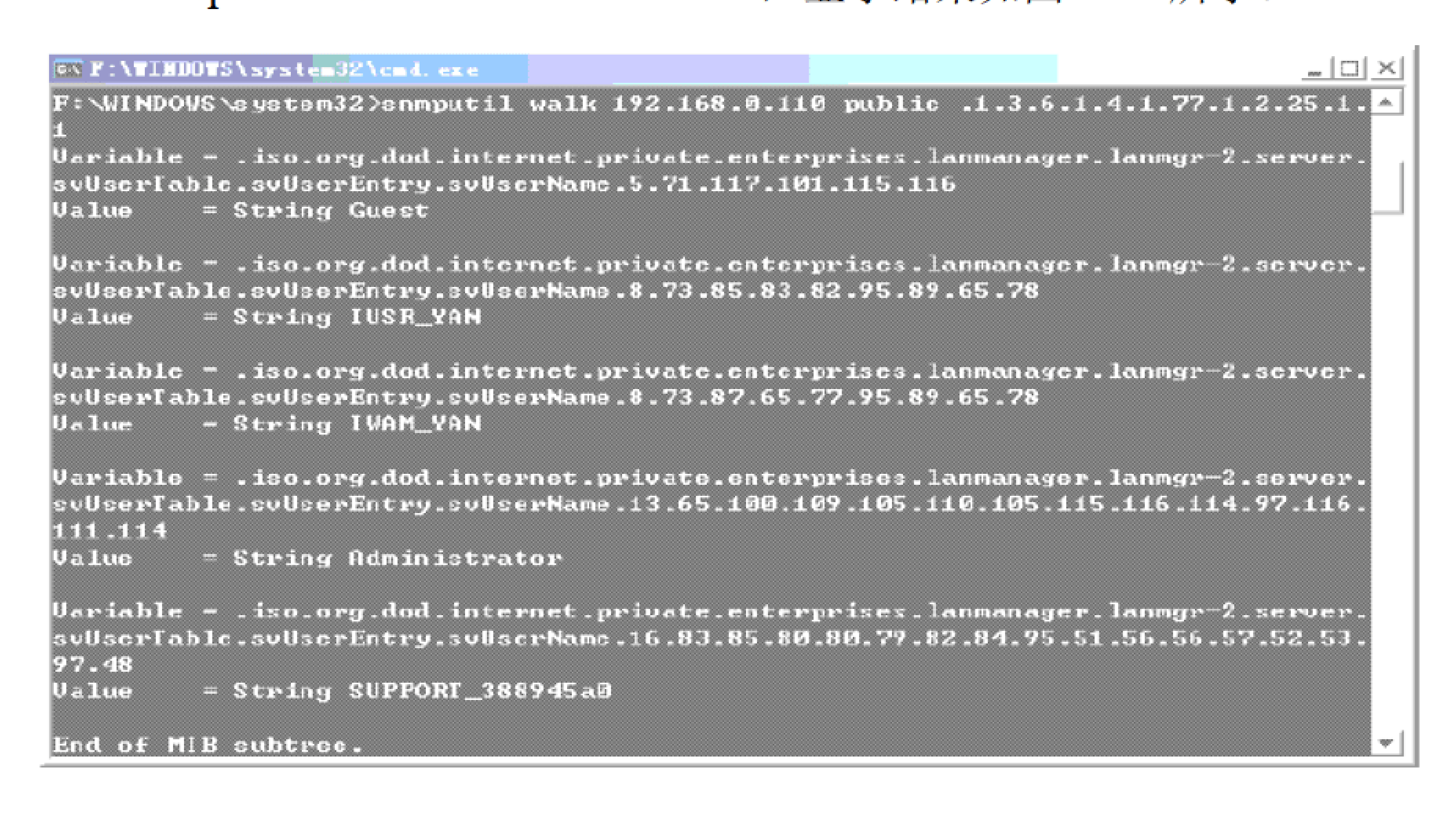


图 4-17　系统输出信息

【问题 1】(4 分)

能够发送 SNMP 请求报文并能对 SNMP 报文进行解析的服务为__(1)__；用以监听被管主机发送来的陷入报文的服务为__(2)__。

(1) A. SNMP Service　　B. Task Scheduler
　C. Terminal Services　　D. SNMP Trap Service

(2) A. SNMP Service　　B. Task Scheduler
　C. Terminal Services　　D. SNMP Trap Service

【问题 2】(4 分)

从图 4-17 可以看出，在图 4-15 所示的界面中，【团体名称】的值应配置为__(3)__；在图 4-16 所示的界面中，还应加入的 IP 地址为__(4)__。

【问题 3】(4 分)

命令 snmputil walk 192.168.0.110 public .1.3.6.1.4.1.77.1.2.25.1.1 的作用是列出被管理对象的__(5)__；命令中的“.1.3.6.1.4.1.77.1.2.25.1.1”表示__(6)__。

(5) A. 系统用户　B. 系统进程　C. 域名　D. 安装的软件

(6) A. 对象　B. 对象标识符　C. 进程编号　D. 值

【问题 4】(3 分)

查询变量 sysDesc 的命令为：snmputil get 192.168.0.110 public 1.1.0，采用下列命令：

snmputil __(7)__ 192.168.0.110 public 1.1，也可以达到查询变量 sysDesc 的目的。

A. get　　B. getnext　　C. set　　D. trap

分析：

【问题 1】

Windows 的 SNMP 服务包括两个应用程序。一个是 SNMP 代理服务程序 Snmp.exe，另一个是 SNMP 陷入服务程序 snmpTrap.exe。Snmp.exe 接收 SNMP 请求报文，根据要求发送响应报文，能对 SNMP 报文进行语法分析，对 ASN.1 和 BER 编码/译码，也能发送陷入报文，并处理与 WinSock API 的接口，Windows 98 也含有这个文件。snmpTrap.exe 监听发送给 NT 主机的陷入报文，然后把其中的数据传送给 SNMP 管理 API，Windows 98 没有该陷入服务文件。故(1)、(2)处分别应选 A、D。

【问题 2】

snmputil 的用法如下：

usage:snmputil [get | getnext | walk]agentaddresscommunityoid[oid…]snmputil trap

从图 4-17 可以看出，输入的命令为 snmputil walk192.168.0.110 public.1.3.6.1.4.1.77.1.2.25.1.1，因此团体名称应为 public，故(3)处应填入 public；被查询主机的 IP 地址为 192.168.0.110，故(4)处应填入 192.168.0.110。

【问题 3】

从图中可以看出，命令 snmputil walk192.168.0.110 public.1.3.6.1.4.1.77.1.2.25.1.1 的作用是列出被管理对象的系统用户；命令中的“.1.3.6.1.4.1.77.1.2.25.1.1”表示被查询对象的对象标识符，即 oid。故(5)、(6)处应分别选择 A、B。

【问题 4】

采用 snmputil getnext 192.168.0.110 public 1.1 命令可以达到 snmputil get 192.168.0.110 public 1.1.0 命令的目的。故(7)处应选择 B。

答案：

【问题 1】

(1) A　　(2) D

【问题 2】

(3) public　　(4) 192.168.0.110

【问题 3】

(5) A　　(6) B

【问题 4】

(7) B

例 7　阅读以下说明，回答问题 1～问题 3，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题一)

【说明】

某公司总部和三个子公司分别位于四处，网络结构如图 4-18 所示，公司总部和各子公司所需主机数如表 4-3 所示。

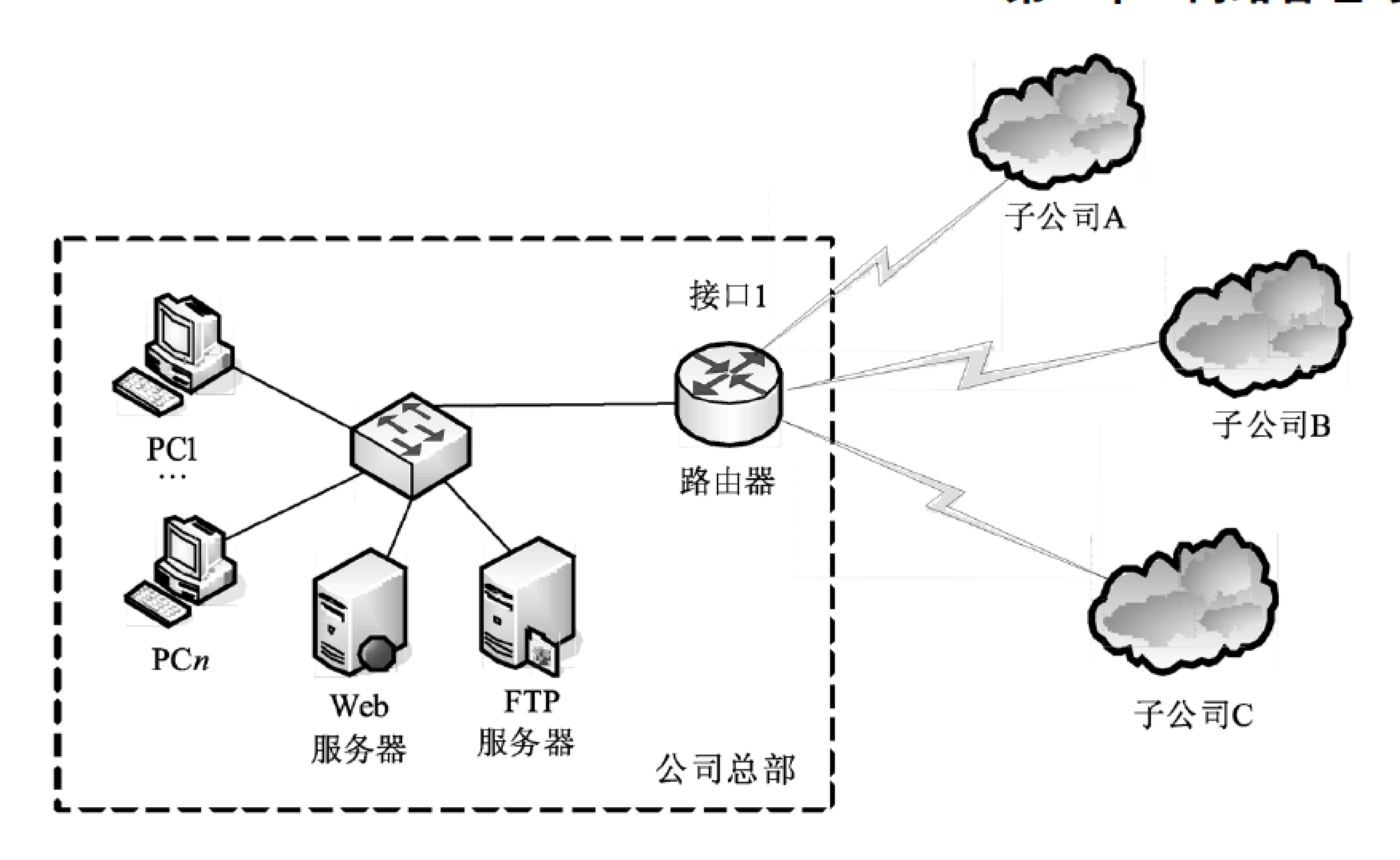


图 4-18　某公司网络拓扑结构

表 4-3　各公司所需的主机数

部　门	主机数量/台
公司总部	50
子公司 A	25
子公司 B	10
子公司 C	10

【问题 1】(7 分)

发现子公司 A 的某台 PC 无法访问 Web 服务器，作如下检查。

① 查看【网上邻居】，发现该 PC 可以访问子公司 A 内其他主机。

② 采用__(1)__命令来检查与路由器接口 1 的连通性，结果正常。

③ 该 PC 可以通过域名访问 FTP 服务器。

④ 用 SHOW ACCESS-LIST 命令检查路由器的__(2)__，发现有问题，那么造成该 PC 无法访问 Web 服务器的原因可能是__(3)__。

(1) A．ping　　B．nslookup　　C．netstat　　D．interface

(2) A．地址解析协议　　B．访问控制列表　　C．路由表　　D．IP 地址

(3) A．该 PC 子网掩码配置错误

B．该 PC 网关配置错误

C．该 PC 的 DNS 服务器地址配置错误

D．路由器对该 PC 访问 Web 服务器的权限进行了限制

【问题 3】(2 分)

可以采用__(4)__方法防止 IP 地址被盗用。

A．IP 地址与子网掩码进行绑定　　B．IP 地址与 MAC 地址进行绑定

C．设置网关地址　　D．IP 地址与路由器地址进行绑定

分析：

【问题 1】

通过以上描述，可以得出以下结论：①既然能看到一部分电脑，说明网络连接正常，而且正确安装了网卡驱动程序和网络通信协议；②通过 ping 测试网关地址正常，通过域名可访问 FTP 服务器，说明 IP 地址、子网掩码、网关、DNS 信息设置正确；③用 SHOW ACCESS-LIST 命令检查路由器的访问控制列表有问题，说明造成该 PC 无法访问 Web 服务器的原因可能是路由器对该 PC 访问 Web 服务器的权限进行了限制。

【问题 2】

为了防止 IP 地址被盗用，在路由器上可将某台机器的 MAC 地址与 IP 地址绑定。

答案：

【问题 1】

(1) A　　(2) B　　(3) D

【问题 2】

(4) B

4.2.3 同步练习

1. 某公司内部有一个采用 TCP/IP 作为传输协议的 100Base-TX 局域网，包括一台服务器和 20 台客户机，通过一台 16 端口的交换机与一台 8 端口共享集线器级联，其网络结构如图 4-19 所示。服务器上运行 DHCP 服务软件，客户机的 IP 地址由 DHCP 服务程序自动分配。主机 B 登录网络后在网络邻居中只能看到自己的主机名，而看不到服务器和其他客户机的主机名，列出可能出现的硬件和软件故障。

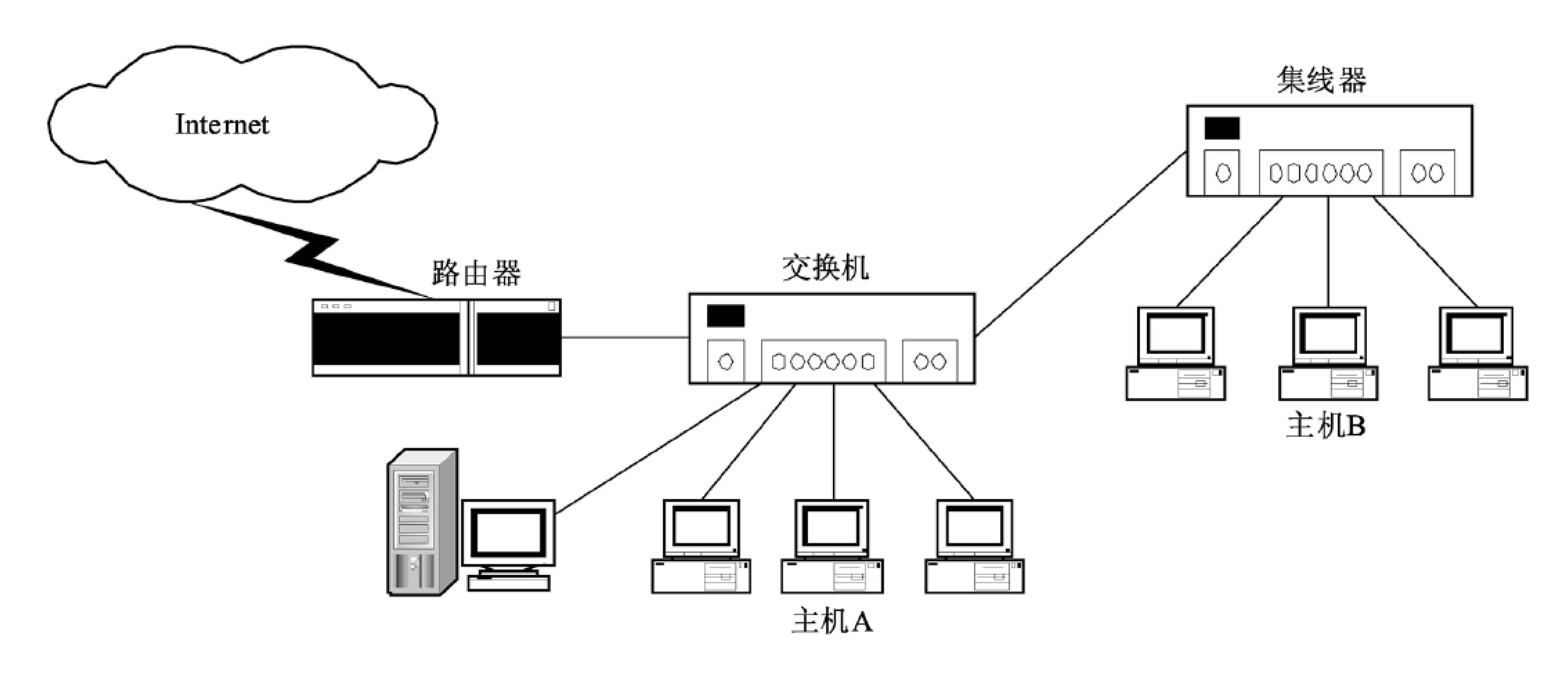


图 4-19　某公司网络结构

2. 有一小型局域网，服务器为 Windows NT 操作系统，各工作站为 Windows 98 操作系统。以前局域网一直工作正常，后来有一台工作站重新安装 Windows 98 之后，这台电脑通过网上邻居浏览其他电脑的速度非常慢，而且只能看到一部分电脑，有的电脑却看不到，

而其他电脑相互之间一切正常。检查 IP 地址与子网掩码没有错误，域名与工作组也相同。列出可能出现该问题的原因。

3．有一台 PC 无法访问其他计算机和 Internet，通过 ping 命令 ping 127.0.0.1 成功，ping 自己的网卡地址却不成功。请列出可能出现的故障原因。

4．有一台客户机，能够通过网上邻居看到其他客户机和服务器，但就无法访问到 Internet(通过 IP 地址也不行)，但其他客户机却可以。请问最有可能的原因是什么？

5．某公司的域名为 abc.com.cn，内部有一个名字为 www.abc.com.cn 的 Web 服务器，有一台客户机在浏览地址栏中输入 www.abc.com.cn 却无法访问内部的 Web 服务器，输入 Web 服务器的 IP 地址却可以访问，但其他客户机却可以。请问最有可能的原因是什么？

6．网络配置如下：两个子网，一个路由器。路由器有两个接口：网络 A 为 167.191.32.1，网络 B 为 167.191.64.1，所有计算机使用一个子网掩码 255.255.224.0。你的 Windows 2000 工作站连接不到网络 A 上的远程服务器，但网络 B 上所有其他工作站都能连接上。你的工作站位于网络 B。当在工作站上运行 ipconfig/all 命令时，接收到如下输出。

IP 地址是 167.191.82.17；子网掩码是 255.255.224.0；默认网关是 167.191.32.1。导致这一问题的最可能原因是什么?

4.2.4　同步练习参考答案

1. 硬件故障主要有：网卡故障、通信介质故障(包括网线、跳线或信息插座故障)、Hub 硬件故障(包括 Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障)，软件故障包括：网卡驱动程序未安装或安装不正确，网络协议未安装或设置不正确，DHCP 服务器设置错误或 IP 地址资源不足。

2. 没有安装 NetBEUI 协议、网卡驱动程序有问题、Windows NT 没有活动目录功能。

3．网卡坏了、IP 地址与其他主机冲突。

4．默认网关没有设置或设置不正确。

5．TCP/IP 属性的 DNS 服务器设置错误或没设置。

6．错误的默认网关，默认网关应当为 167.191.64.1。

4.3　本 章 小 结

本章知识点在 2009 年的新大纲中基本没有改变，只是一些表述方式的调整。

这部分主要介绍了常用网络工具的使用；简单网络故障的分析、定位、诊断和排除。

本章内容为下午科目的重点内容，尤其是网络管理命令。本章的每小节中都组织了一些针对水平考试的典型例题分析和同步训练，这些题目基本上涵盖了大纲规定的知识要点。

4.4 达标训练题及参考答案

4.4.1 达标训练题

1．ping 命令的“-n count”参数的含义是什么？

2．命令“netstat -s -p TCP 60”的含义是什么？

3．有一小型局域网，一台服务器用作 DHCP 服务器，为各客户机分配 IP 地址，有 20 台客户机，它们通过一台 24 口 Hub 相连。有一台 Windows 2000 客户机启动时无法访问 Internet，运行 ipconfig/all 命令后显示 MAC 地址为 00-00-E8-6E-24-2F，IP 地址为 0.0.0.0，子网掩码为 0.0.0.0，DHCP 服务器地址是 255.255.255.255。请列出可能出现的硬件和软件故障。

4．某一公司的域名为 abc.com.cn，内部有一个名字为 www.abc.com.cn 的 Web 服务器，所有客户机在浏览地址栏中输入 www.abc.com.cn 都无法访问内部的 Web 服务器。请问最有可能的问题是什么？

4.4.2 参考答案

1．指定要 ping 多少次，具体次数由 count 来指定。

2．每分钟统计一下本机的 TCP 连接情况。

3．硬件故障主要有：网线、跳线或信息插座故障、Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障；软件故障主要是 DHCP 服务器设置错误或 IP 地址资源不足，客户机无法租约到 IP 地址。

4．域名服务器工作不正常或配置错误。

第 5 章　Web 网站建设

大纲要求：

- Web 网络的规划、建立、管理与维护
- 使用 HTML 进行网页设计与制作
- JSP、ASP 动态网页编程技术
- ADO 的概念和使用

5.1　用 HTML 制作网页

5.1.1　考点辅导

5.1.1.1　HTML 简介

HTML(Hyper Text Mark-up Language，超文本标记语言)是 WWW 的描述语言。它是标准通用型标记语言(Standard Generalized Markup Language，SGML)的一个应用。

1. HTML 元素

HTML 是标准的 ASCII 文档。其扩展名通常是.html、.htm、.mht、.mhtml 或.shtml，这是常见的 5 种格式。从结构上讲，HTML 由元素组成，它用成对的标签(Tag)，即起始标签和结束标签来组织和定义文档的显示格式。HTML 文件中 HTML 标签的语法格式如下：

<标签名称>标签对象</标签名称>

2. HTML 文档的组成

HTML 文档以<html>标签开始，以</html>标签结束，由文档头和文档体两部分构成。文档头以<head>标签开始，以</head>标签结束；文档体以<body>标签开始，以</body>标签结束。

文档头部分可以包含以下元素。

(1) 窗口标题。是对 HTML 文档的简单描述，对应标签为<title></title>。

(2) 脚本语言。是指浏览器解释执行的语句，对应标签为<script></script>。

(3) 样式定义。样式表主要用于格式化网页中的元素，对应标签为<style></style>。

(4) 元数据。主要提供超文本文档内容和主题的信息，对应标签为<meta>。

文档体包含了可以在浏览器中显示的内容，包含以下元素。

(1) 文本。文本通常以格式化的内容放在文档体中。

(2) 图像。图像主要用于丰富网页的内容。

(3) 链接。链接通常放在文档体中，允许在网站中导航到其他网站。

(4) 多媒体和特定的编程事件。主要是指包含在 HTML 文档中的 Shockwave、Java

Applet 或在线视频等。

3. HTML 文档的结构

HTML 文档的基本结构如下：

```
<html>
<head>
<title> </title>
…
</head>
<body>
…
</body>
</html>
```

5.1.1.2 HTML 常用元素

1. 基本元素

1) 窗口标题(Title)

Title 是 HTML 文档的标题，是对文档内容的概括，在 Web 面浏览时，它出现在浏览器的标题栏。其使用格式为

```
<title>窗口标题描述</title>
```

2) 页面标题

页面标题有 6 种，分别为 h1、h2、h3、h4、h5 和 h6，用于表示页面中的各种标题。其使用格式为

```
<hn >页面标题描述</hn> (n=1, 2, …, 6)
```

标题可以有对齐属性 align，其属性值有 left(标题居左)、center(标题居中)和 right(标题居右)等。例如：

```
<h2 align="center">居中的二级页面标题</h2>
```

3) 字体

HTML 的字体包括字体大小、字体风格、字体颜色和闪烁等。

字体大小：HTML 有 7 种字号，1 号最小，7 号最大，默认字号为 3。可以用<basefont size=字号>设置默认字号。

字体风格：字体主要包括以黑体<b>、斜体<i>和下画线<u>为代表的物理风格以及特别强调<strong>、源代码<code>和例子<samp>等为代表的逻辑风格。

字体颜色：字体颜色用<font color=#>指定，#可以是 6 位的十六进制数，也可以是 black、navy 和 purple 等英文颜色名称。

闪烁：标签<blink>文本</blink>使文本闪烁，闪烁频率为 1 秒一次。

4) 横线

横线，也称水平线，一般用于分隔文本。其 HTML 标签为<hr>。可以指定水平线的对齐、颜色、阴影和高度等相关属性。例如：

```
<hr  align="center" color=blue  noshade  size="1">
```

表示设定水平线的格式为：居中对齐，蓝色，无阴影，高度为 1。

5) 分行和禁止分行

HTML 标签
，表示在此处分行。<nobr>…</nobr>通知浏览器：其中的内容在一行内显示，若一行显示不了，则超出部分被裁剪。

6) 分段

HTML 的分段完全依赖于分段标签<p>段落文本</p>。<p>也可以设定对齐、风格等。例如：

```
<p align="left"  style="color:#FF0000 ">
```

表示该段落格式为左对齐，字体颜色为红色。

7) 转义字符与特殊字符

HTML 使用的字符集是 ISO ＆859 Larin-1 字符集，该字符集中有许多标准键盘上无法输入的字符。对于这些字符只能使用转义字符。常见的需要转义的字符有<、>、&和引号等。

“<”的转义序列为&lt 或&#60；“>”的转义序列为&gt 或&#62；引号的转义序列为&quot 或&#34。例如：

```
<img src="pictures/tower.jpg" alt="安庆府&quot;镇风塔&quot">
```

注意： 转义序列各字符间不能有空格；转义字符必须以“;”结束；单独的&不被认为是转义的开始。

8) 背景和文本颜色

窗口背景和文本可以使用以下标签指定：

```
<body background="image-URL"></body>
<body bgcolor="#" text="#" link="# " alink="# " vlink="# "></body>
```

其中，background 表示背景图片；image-URL 代表背景图片的 URL 地址；bgcolor 是指背景颜色，其中#后面是指定的十六进制的红、绿、蓝分量；text 表示文本颜色；link 表示链接颜色；alink 表示活动链接颜色；vlink 表示已访问过的链接颜色。

例如：

```
<body background="images/bg.gif" bgcolor="#FFFFFF" text="#000000"
link="#FF0000" alink="#0000FF" vlink="#FF00FF" ></body>
```

表示页面背景图片是 images 文件夹下的 bg.gif 文件，页面背景颜色为白色，文本颜色为黑色，链接颜色为红色，活动链接为蓝色，已访问过链接为粉红色。

9) 图像

图像(Image)主要用于网页美工。

其使用的基本格式为：

```
<img src="image-URL" width="#" height="#">
```

其中，image-URL 是图像文件的 URL；width 和 height 表示图像文件的宽度和高度。

另外，可选的图像属性还包括 alt、align 以及 vspace 和 hspace 等。其中，alt 是指图像的替代文字；align 指图像的对齐属性；vspace 和 hspace 表示文本与图像的纵向和横向间距。

例如：

```
<img src="pictures/tower.jpg" width="200" height="100" align="middle" alt=
"镇风塔" vspace="50" hspace="50">
```

10) 列表

列表(List)主要用于列举条目。常用的列表有 3 种格式，即无序列表、有序列表和自定义列表。

(1) 无序列表：以
开始，每一列表条目用
引导，黑点表示，最后是。例如：

```
<ul>
<li>昨天</li>
<li>今天</li>
<li>明天</li>
</ul>
```

(2) 有序列表：以
开始，每一列表条目用
引导，数字表示，最后是。例如：

```
<ol>
<li>昨天</li>
<li>今天</li>
<li>明天</li>
</ol>
```

(3) 自定义列表：以<dl>开始，每一列表条目用<dt>引导，说明用</dd>表示，最后是</dl>。例如：

```
<dl>
<dt>昨天</dt>
<dd>yesterday</dd>
<dt>今天</dt>
<dd>today</dd>
</dl>
```

2. 超文本链接

超文本链接，一般由两部分组成：一是被指向的目标，二是指向目标的链接。

1) 统一资源定位器 URL

用于指定访问文档的方法。一个 URL 的构成为：

```
Protocol://machine.name[:port]/directory/filename
```

其中，Protocol 是指访问该资源所采用的协议，它可以是 HTTP(超文本传输控制协议)、FTP(文件传输控制协议)或 NEWS(网络新闻资源)等；machine.name 是指存放资源的主机 IP；port 是指用于存放资源的主机的相关服务的端口号；directory 和 filename 是该资源的路径和文件名。

例如：

```
http://www.microsoft.com
```

2)　超级链接标签

在 HTML 文档中用链接指向一个目标。其基本格式为

```
<a href="URL">字符串</a>
```

例如：

```
<a href="http://www.yahoo.com ">雅虎搜索</a>
```

3)　标记

标记，也可称为书签或锚记。标识一个链接目标的方法为：

```
<a name="name">text</a>
```

其中，name 属性放置 HTML 文档的全文惟一的标记串，可以用下列方法来指向它。

```
<a href="URL#name">text</a>
```

例如：

```
<a href="http://www.sina.com.cn/sports/news.htm# import">欧洲赛事</a>
```

4)　图像链接

图像也可以建立超级链接。其格式为

```
<a href="URL "><img src="URL "> </a>
```

例如：

```
<a href="http://www.macromedia.com"><img src="macromedia.gif" ></a>
```

5)　图像地图

图像地图可以把图像分成多个区域，每一区域指向不同的目标。图像地图可以分为服务器端和客户端地图。服务器端的使用格式为

```
<a href="/cgi-bin/imagemap/mymap.map">
<img src="mymap.gif" ismap></a>
```

其中，mymap.map 是存放在服务器端/cgi-bin 目录下的图像地图的分区信息文件。

客户端图像地图的使用格式为

```
<img src="image-URL" usemap="#">
```

其中，image-URL 为用作图像地图的图像，usemap 指客户端地图的标记名。

客户端图像地图的分区信息用<map name=mapname>说明。图像地图的各个区域用<area shape="形状" coords="坐标" href="URL">说明。形状可以是矩形、圆形或多边形。

例如：

```
<img src="map.gif" usemap="#Map">
<map name="Map">
 <area shape="rect" coords="74,100,150,184" href="first.htm">
 <area shape="circle" coords="314,230,65" href=" second.htm ">
```

```
 <area shape="poly" coords="39,357,166,369,183,313,129,263,49,304"
href="third.htm ">
</map>
```

3. 表格

表格(Table)通常用于组织和排列网页信息。表由<table >开始，</table >结束。表的内容由<thead>、<tbody>、<th>、<tr>和<td>定义。

其基本格式为

```
<table >
  <thead>
  <tr>
  <th>… </th>
   …
  </tr>
  </thead>
  <tbody>
   <tr>
    <td>…</td>
    …
  </tr>
   …
  </tbody>
</table>
```

其中，<thead>是表头标签，<tbody>是表格的主体，<th>是列标题标签，<tr>是表中的行标签，<td>是表中的列标签。表 5-1 中列出了 table 标签中的一些属性值及其描述。

表 5-1　table 标签中的一些属性值及其描述

属　性	值	描　述
align	left ,center ,right	规定表格相对周围元素的对齐方式
bgcolor	rgb(x,x,x)	规定表格的背景颜色
border	pixels	规定表格边框的宽度
cellpadding	pixels ,%	规定单元格边沿与其内容之间的空白
cellspacing	pixels, %	规定单元格之间的空白
width	pixels ,%	规定表格的宽度
height	pixels ,%	规定表格的高度

4. 框架

框架(Frame)将浏览器的窗口分成多个区域，每个区域可以单独显示一个 HTML 文档，各个区域的文档可以关联地显示相关内容。

框架的基本结构如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
```

```
<title>… </title>
</head>
<frameset >
  <frame src="URL" name="leftFrame" >
  <frame src="URL" name="mainFrame">
…
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

框架中可以放置相应的 HTML 页面，主要是通过以下标签来完成的。

1)　<frameset >标签

框架集标签，基本参数包括 frameborder、border 和 framespacing 等，主要用于定义整个框架集的行列及边界参数。

2)　<frame >标签

单独框架标签，基本参数包括 src 和 name 等，主要用于指定填充该框架的 HTML 文档属性。

3)　<noframe >标签

当浏览器不支持框架时就显示该标签中的内容。

例如：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>上方固定左侧嵌套</title>
</head>
<frameset rows="80,*" cols="*" frameborder="NO" border="0"
framespacing="0">
  <frame src="top.htm" name="topFrame" scrolling="NO" noresize >
  <frameset cols="80,*" frameborder="NO" border="0" framespacing="0">
    <frame src="left..htm" name="leftFrame" scrolling="NO" noresize>
    <frame src="main.htm" name="mainFrame">
  </frameset>
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

5.　表单

表单(Form)是网页中一种重要的信息收集和交流工具，它在 Web 数据库技术中起着关键性作用。下面是一个包含简单表单对象的 HTML 文本的示例。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>百度搜索</title>
</head>
<body>
<FORM name=f action=http://www.baidu.com/baidu  method="post"><INPUT
class=ff
     maxLength=100 size=35 name=w>
  <INPUT type=submit value=百度搜索>
</FORM> </FORM>
</body>
</html>
```

1) 表单标签

标签<FORM>提供表单的功能，由开始和结束标签<FORM>…和</FORM>组成，表单中可以设置文本框、按钮或下拉菜单等表单域元素。在开始标签中带有两个重要属性：ACTION 和 METHOD，分别指定了表单的动作和方法。

2) 文本框

文本框可以分为单行文本框和多行文本框。单行文本框的 HTML 基本标签是：<input type="text" name="textfield">；多行文本框的 HTML 基本标签是：<textarea name="textfield"></textarea>。

3) 按钮

按钮可以分为单选按钮、复选框以及提交和重置按钮。单选按钮的 HTML 基本标签是：<input type="radio" name="radiobutton" value="radiobutton">；复选框的 HTML 基本标签是：<input type="checkbox" name="checkbox" value="checkbox">；提交和重置按钮的 HTML 基本标签分别是：<input type="submit" name="Submit" value="提交">和<input type="reset" name="Submit" value="重置">。

4) 下拉菜单

下拉菜单通过标签<select>实现，其 HTML 基本标签是：<select name="select" size="1"></select>。

表 5-2 列出了表单常用的控件、常用属性及属性值。

表 5-2 表单常用的控件、常用属性及属性值

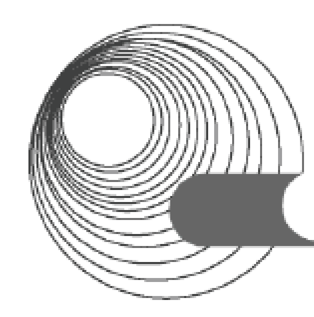
控件名	主要属性	属性值
文本框	name	任意
	type	text
	value	任意(表单实际的值)
	size	数字(文本框的长度)
	maxlength	数字(文本框的最大长度)

续表

控 件 名	主要属性	属 性 值
文本域	name	任意
	type	textarea
	cols	数字(文本域列数)
	rows	数字(文本域行数)
单选按钮	name	任意
	type	radio
	value	任意(表单实际的值)
	checked	checked(表示单选按钮默认选中)
复选框	name	任意
	type	checkbook
	value	任意(表单实际的值)
	checked	checked(表示复选框默认选中)
下拉列表框	name	任意
	type	select
	size	数字(下拉列表框高度)
下拉列表选项	type	option
	vlaue	任意(表单实际的值)
	selected	selected(该选项默认被选中)
密码	name	任意
	type	password
	value	任意(表单实际的值)
提交按钮	name	任意
	type	sumbit
	value	任意(按钮实际的值)
重置按钮	name	任意
	type	reset
	value	任意(按钮实际的值)
文件框	name	任意
	type	file
图像	name	任意
	type	image
	src	URL(图片路径)

5.1.1.3　应用实例

以下是著名的 Google 搜索引擎首页的 HTML 源文件。(注：为了方便读者阅读，笔者进行了重新排版。)




```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>Google</TITLE>
<META http-equiv=content-type content="text/html; charset=UTF-8">
<STYLE>
  BODY {FONT-FAMILY: arial,sans-serif}
  TD {FONT-FAMILY: arial,sans-serif }
  A {FONT-FAMILY: arial,sans-serif }
  P {FONT-FAMILY: arial,sans-serif }
 .h {FONT-FAMILY: arial,sans-serif}
 .h {FONT-SIZE: 20px}
 .q {COLOR: #0000cc}
</STYLE>
<SCRIPT>
<!--
  function sf(){document.f.q.focus();}
  function clk(el,ct,cd,sg)
  {  if(document.images)
    {  (new Image()).src="/url?sa=T&ct="+escape(ct)+
        "&cd="+escape(cd)+"&url="+escape(el.href).replace(/\+/g,"%2B")+
        "&ei=WXG6Qs3eO6qmOMPehZwP"+sg;}
      return true;}
  function rbi(f)
  {  if (navigator.appName == "Netscape")
     {  f.biw.value=self.innerWidth;}
     else {  f.biw.value=document.body.clientWidth;}}// -->
</SCRIPT>
<META content="MSHTML 6.00.2900.2135" name=GENERATOR></HEAD>
<BODY text=#000000 vLink=#551a8b aLink=#ff0000 link=#0000cc bgColor=#ffffff
topMargin=3 onload=sf() marginheight="3">
<CENTER>
  <IMG height=110 alt=Google src="logo.gif" width=286>
  <FORM name=f onsubmit=rbi(this); action=/search>
<SCRIPT><!--
 function qs(el)
 {  if (window.RegExp && window.encodeURIComponent)
    { var ue=el.href;var qe=encodeURIComponent(document.f.q.value);
      if(ue.indexOf("q=")!=-1)
      {  el.href=ue.replace(new RegExp("q=[^&$]*"),"q="+qe);}
      else{el.href=ue+"&q="+qe;}
    }
    return 1;}
// -->
</SCRIPT>
<TABLE cellSpacing=0 cellPadding=4 border=0>
  <TBODY>
  <TR>
    <TD noWrap><FONT size=-1><B>网页</B>    
<A class=q id=1a  onclick="return qs(this);"
     href="http://www.google.com/imghp?hl=zh-CN&amp;tab=wi">图片</A>
```

```
<A class=q id=2a onclick="return qs(this);"
     href="http://www.google.com/nwshp?hl=zh-CN&amp;tab=wn">新闻</A>
<A class=q id=3a onclick="return qs(this);"
     href="http://www.google.com/grphp?hl=zh-CN&amp;tab=wg">论坛</A>
<A class=q id=4a onclick="return qs(this);"
  href="http://www.google.com/dirhp?hl=zh-CN&amp;tab=wd">网页目录</A><B>
      <A  class=q  href="http://www.google.com/intl/zh-CN/options/">更多
 »</A></B>
      </FONT></TD></TR></TBODY></TABLE>
<TABLE cellSpacing=0 cellPadding=0>
  <TBODY>
  <TR>
    <TD width="25%"> </TD>
    <TD align=middle>
       <INPUT type=hidden name=biw>
       <INPUT type=hidden  value=zh-CN name=hl>
      <INPUT maxLength=256 size=55 name=q><BR>
      <INPUT type=submit value="Google 搜索" name=btnG>
       <INPUT type=submit value=手气不错 name=btnI></TD>
    <TD vAlign=top noWrap width="25%"><FONT size=-1>  
<A href="http://www.google.com/advanced_search?hl=zh-CN">高级搜索</A><BR>
<A href="http://www.google.com/preferences?hl=zh-CN">使用偏好</A><BR>
<A href="http://www.google.com/language_tools?hl=zh-CN">语言工具</A>
</FONT></TD></TR>
  <TR>
    <TD align=middle colSpan=3><FONT size=-1>
      <INPUT id=all type=radio CHECKED value="" name=lr>
      <LABEL for=all>搜索所有网页</LABEL>
      <INPUT id=ch type=radio value=lang_zh-CN|lang_zh-TW name=lr>
      <LABEL for=ch>搜索所有中文网页</LABEL>
      <INPUT id=il type=radio value=lang_zh-CN name=lr>
      <LABEL for=il>搜索简体中文网页</LABEL>
   </FONT></TD></TR></TBODY></TABLE></FORM>
  <p><FONT size=-1><p></FONT <BR>
  <p><BR><BR><FONT size=-1>
  <A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A> -
  <A href="http://www.google.com/intl/zh-CN/about.html">Google 大全</A> -
  <A href="http://www.google.com/ncr">Google.com in English</A>
  <SPAN id=hp style="BEHAVIOR: url(#default#homepage)"></SPAN>
<SCRIPT>
//<!--
    if (!hp.isHomePage('http://www.google.com/'))
     {  document.write("<p><a href=\"/mgyhp.html\"
         onClick=\"style.behavior='url(#default#homepage)';
   setHomePage('http://www.google.com/');\">将 Google 设为首页! </a>");}
//-->
</SCRIPT>
 </FONT>
<P><FONT size=-1>©2005 Google - 搜索 8,058,044,651 张网页</FONT></P>
```

```
</CENTER></BODY></HTML>
```

该文档在 IE 浏览器中的运行结果如图 5-1 所示。

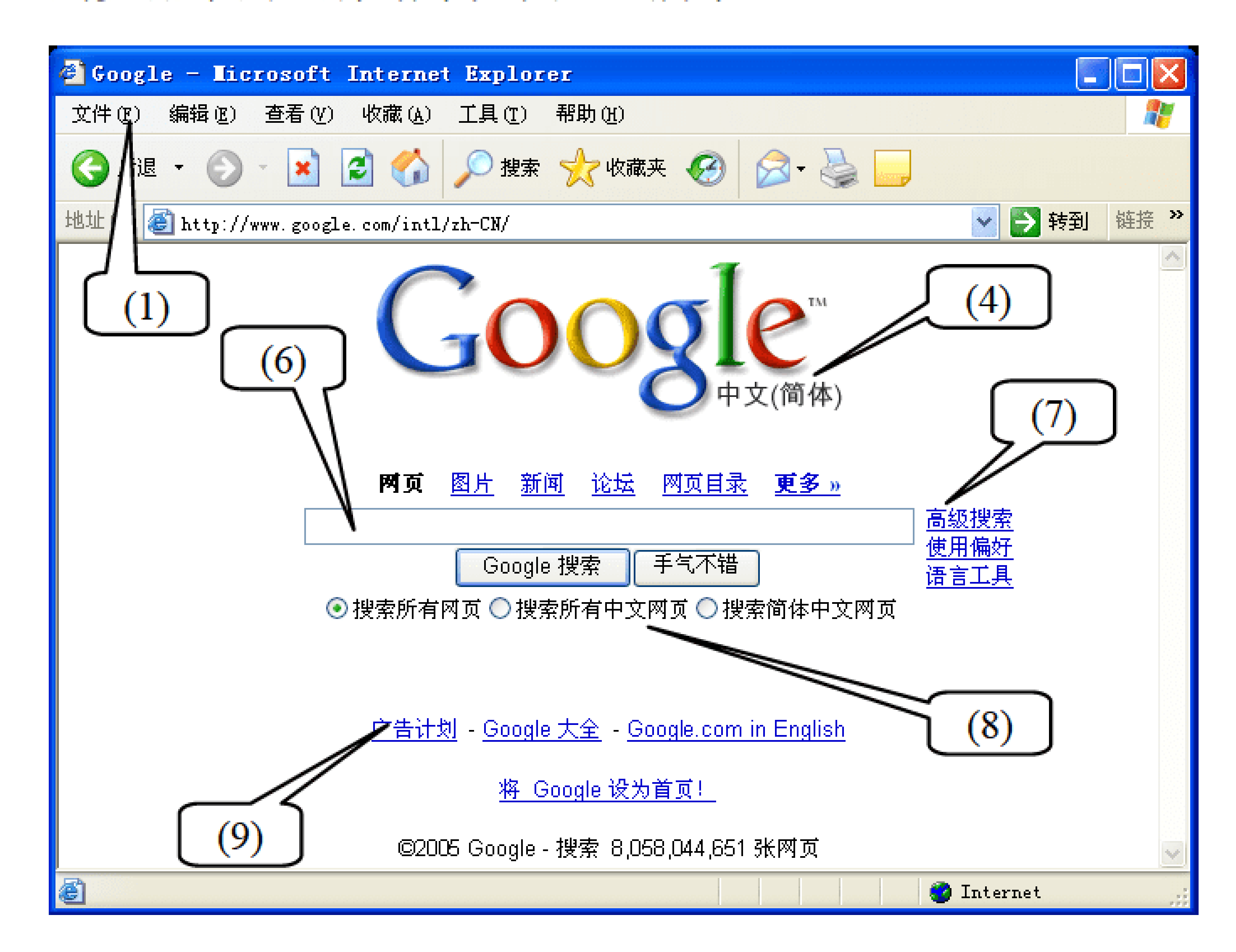


图 5-1　Google 首页

相关 HTML 代码说明如下。

(1) <TITLE>Google</TITLE>，<TITLE>定义网页的标题是 Google。

(2) <STYLE>BODY {FONT-FAMILY: arial,sans-serif}…</STYLE>，<STYLE>定义了网页元素的样式。

(3) <SCRIPT><!--function sf(){…}…// --></SCRIPT>，<SCRIPT>定义了网页使用的 Java Script 的函数。

(4) <IMG height=110 alt=Google src="Google.files/logo.gif" width=286>，<IMG>定义了网页中所使用的 LOGO 图片。

(5) <TABLE cellSpacing=0 cellPadding=4 border=0>…</TABLE>，<TABLE>定义了以表格方式排列的网页数据。

(6) <FORM name=f action=/search>…</FORM>，<FORM>定义了网页中的一个表单对象。

(7) <INPUT type=hidden value=zh-CN name=hl>，<INPUT>定义了一个隐含域类型的网页输入数据。

(8) <LABEL for=ch>搜索所有中文网页</LABEL>，<LABEL>定义了表单中的标签对象。

(9) <A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A>，<A>定义了网页中的一个超级链接地址。

5.1.2　典型例题分析

例 1　阅读下列 HTML 文本和说明，在该 HTML 文本中存在 5 处错误，请指出错误

所在的行号、错误原因以及改正的方法，把解答填入答案的对应栏内。

【说明】

这是一个简单的 HTML 文本，显示作者个人主页的登录界面。

HTML 文本如下：

```
(1) <HTML>
(2) <BODY>
(3) <HEAD>
(4) <META NAME="Author" CONTENT="Brent Heslop，David Holzgang">
(5) </HEAD>
(6) <TITLE TITLE="Authors Home Page">
(7) <!-- MAKE SURE BKGND COLOR IS WHITE -->
(8) <BGCOLOR="white">
(9) <IMG ALT="log.jpg" SRC="Welcome to Authors Home page">
(10) <H2><A HREF="http://WWW.authors.public.com">Authors Home Page </A><H2>
(11) <P>Welcome to the authors Web Site. </P>
(12) </BODY>
(13) <HTML>
```

分析：本题主要考核 HTML 语言的基本概念和元素。

HTML 文档以<HTML>标签开始，以</HTML>标签结束，由文档头和文档体两部分构成。文档头由<HEAD>开始，</HEAD>结束；文档体由<BODY>开始，</BODY>结束。

HTML 元素主要包括基本标签、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题仅仅涉及了部分基本标签和图像等元素。

答案：

① 第(2)行不正确：<BODY>标签的位置不正确。<BODY>和</BODY>作为文档体标签，应该置于<HEAD>和</HEAD>之后。

② 第(6)行不正确：<TITLE>标签的使用不正确。<TITLE >和</TITLE >用于定义网页的标题，两个标签之间为标题的内容；并且<TITLE >和</TITLE >标签应位于<HEAD >和</HEAD >标签之间。

③ 第(8)行不正确：<BGCOLOR="white">使用不正确。网页背景是通过<BODY>标签的 BGCOLOR 属性指定，如< BODY BGCOLOR="white">。

④ 第(9)行不正确：<IMG ALT="log.jpg" SRC="Welcome to Authors Home page">使用不正确。<IMG>标签的 ALT 属性是指替代文本，SRC 属性是指图片源文件，因此 ALT 属性值和 SRC 属性值应该对调。

⑤ 第(10)行不正确：<H2> 二级标题标签和<A>超级链接标签的顺序不正确，应该调整为<A HREF="http://WWW.authors.public.com"><H2>Authors Home Page <H2></A>。

例 2　阅读下列说明和 HTML 文本。在 HTML 文本中存在 5 处错误，请指出错误之处并给出改正的方法。

【说明】

这是一个简单的 HTML 文本，描述了框架的 HTML 语法，显示效果如图 5-2 所示。

HTML 文本如下：

```
(1)<html>
(2)<head>
(3)<title>框架测试</title>
(4)</head>
(5)<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
(6)<frameset rows="64, *">
(7)<frame name="banner"scrolling="no"target="contents"src="header.htm">
(8)<frame name="contents" target="list" src="list.htm">
(9)<frameset cols="150, *">
(10)<frame name="main" src="context.htm">
(11)</frameset>
(12)</frameset>
(13)<noframes>
(14)<body><p>此网页使用了框架。</body>
(15)</noframes>
(16)</html>
```

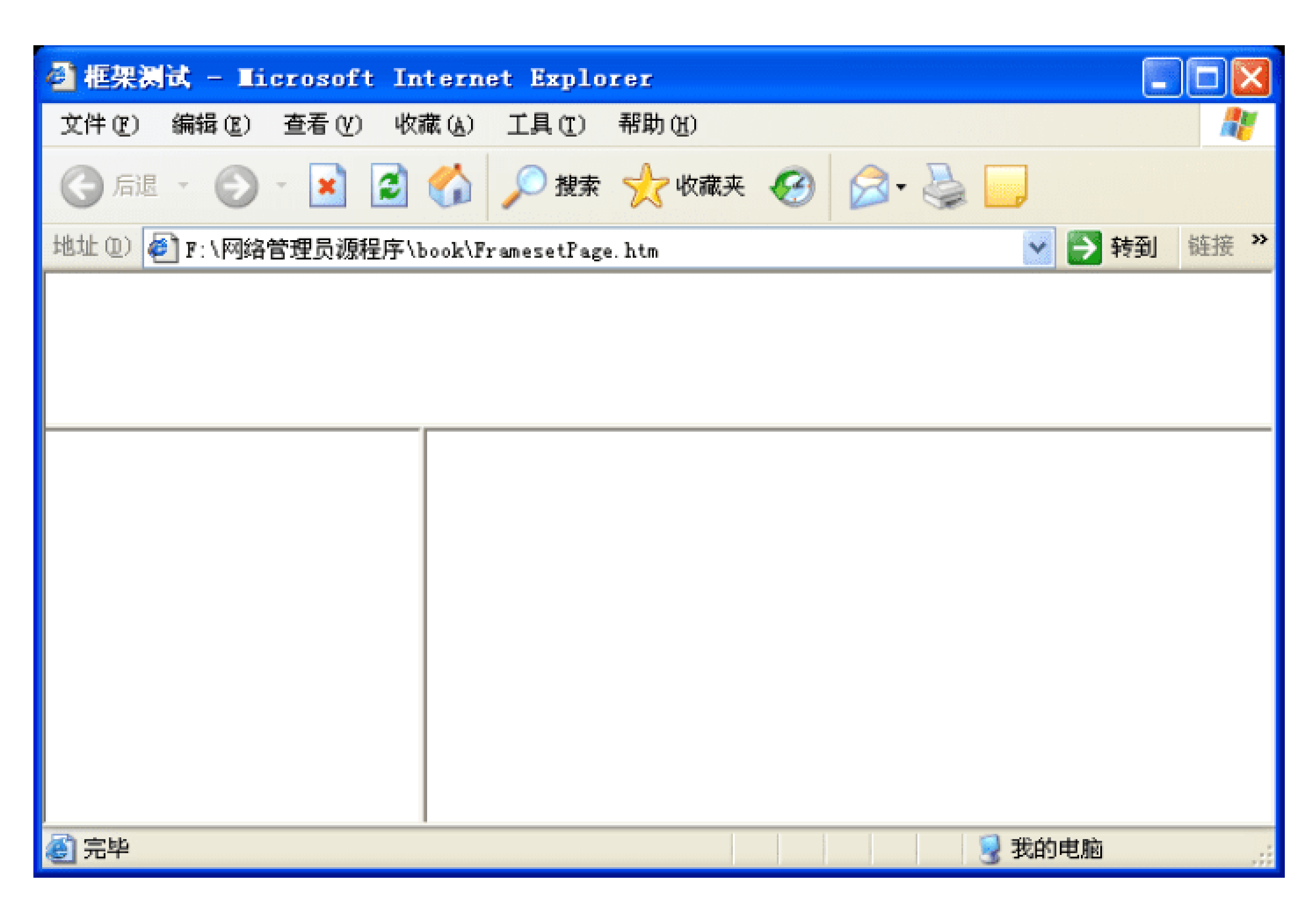


图 5-2　HTML 框架效果

分析：本题主要考查考生对 HTML 文档和框架网页结构的掌握情况。<frameset>标签是一个框架容器，它可以将窗口分成若干个框架，框架的 HTML 标签是<frame>。<frame>的个数是由<frameset>标签中的参数决定的。<frameset>标签中还可能包含一个可选的<noframes>标签，其作用是，当浏览器不支持或禁用<frame>时，<noframes>标签将提供替代的浏览内容。

答案：

① 第(5)行位置不正确：<meta>标签必须位于<head>与</head>标签之间。

② 第(8)行不正确：在<frame>的 target 属性中指定的框架“list”在文本中没有定义，可以改为 banner、contents 或 main 三个中的任何一个。

③ 第(9)行位置不正确：根据图像分析，框架结构应该为上左右型，而本例为左右下

型，应将第(8)、(9)行互调。

④　第(13)、(14)、(15)行位置不正确：<noframes>与</noframes>应位于<frameset>与</frameset>之间。

⑤　第(14)行不正确：<p>与</p>应该成对出现，在文字与</body>之间应添加</p>。

5.1.3　同步练习

阅读下面 HTML 文本和说明，在 HTML 文本中存在 5 处错误，请指出这些错误并给出改正的方法。

【说明】

这是一个简单的 HTML 文档，显示的是一个网页列表信息，显示界面如图 5-3 所示。

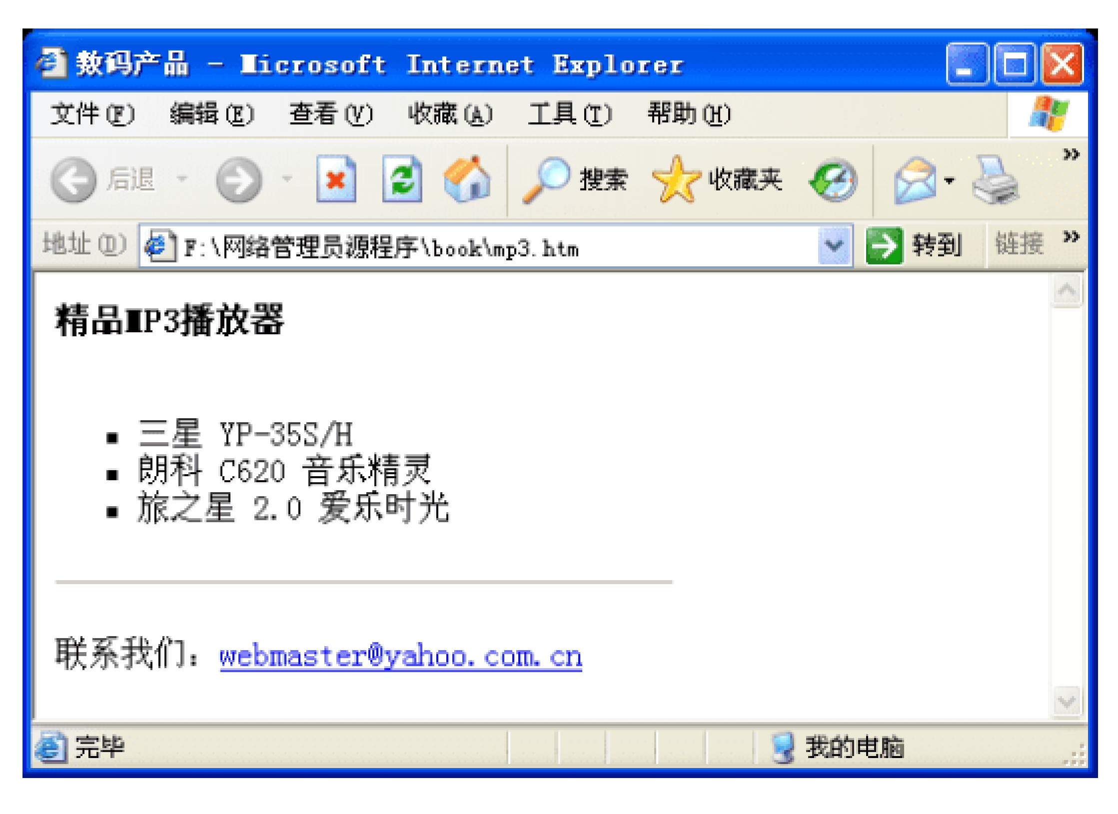


图 5-3　网页列表

HTML 文本如下：

```
(1)<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
(2)"http://www.w3.org/TR/html4/loose.dtd">
(3)<html>
(4)<head>
(5)<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
(6) </head>
(7) <title>数码产品</title>
(8)<body>
(9)<p><strong>精品 MP3 播放器</p></strong>
(10)  <ul type="square">
(11)  <li>三星 YP-35S/H</li>
(12)    <li>朗科 C620 音乐精灵</li>
(13)  </ul>
(14)    <li>旅之星 2.0 爱乐时光</li>
(15) <hr align="left" width="300" size="1">
(16)<p>联系我们:
(17)<a href="mailto:webmaster@yahoo.com"> </a> webmaster@yahoo.com.cn </p>
(18) </html>
(19) </body>
```

5.1.4 同步练习参考答案

① 第(7)行不正确：<title>标签必须位于<head>与</head>标签之间。
② 第(9)行不正确：标签必须位于<p>与</p>之间。
③ 第(13)、(14)行位置不正确：根据图像分析，应将第(13)、(14)行互换。
④ 第(17)行不正确：</p>之前的 webmaster@yahoo.com.cn 应置于之前。
⑤ 第(18)、(19)行位置不正确：根据图像分析，应将第(18)、(19)行互换。

5.2 动态网页制作

5.2.1 考点辅导

动态网页技术主要依赖服务器端编辑，包括 CGI 版本、Server-API 程序(NSAPI 和 ISAPI)、JavaServerlets 以及服务器脚本语言。

服务器脚本环境有许多，其中最流行的几种包括 ASP(Active Server Pages)、ASP.NET(基于.NET 架构的 ASP)、JSP(Java Server Pages)、PHP 等。

5.2.1.1 ASP

1. ASP 简介

1) 什么是 ASP

ASP 是 Active Server Pages(动态服务器页面)的缩写，ASP 可以混合使用 HTML、脚本语言以及组件来创建服务器端功能强大的 Internet 应用程序。ASP 使用 Microsoft 的 ActiveX 技术，它采用封装程序调用对象的技术，从而简化了编程并且加强程序间的协作。

2) ASP 的特点

ASP 运行在服务器端时，不需要编译，可在服务器端直接执行，与浏览器无关。ASP 返回标准的 HTML 页面，浏览者查看页面源文件时，看到的是 ASP 生成的 HTML 代码，而不是 ASP 程序代码。

3) ASP 的编程环境

ASP 的编程语言可以是 VBScript 和 JavaScript，而 VBScript 则是系统默认的脚本语言。ASP 的编程语言可以使用普通的文本编辑器进行设计，ASP 程序则以扩展名.asp 的纯文本形式保存在 Web 服务器上的具有可执行权限的虚拟目录之下，供用户通过 WWW 的方式访问。

2. ASP 内嵌对象

ASP 提供了可以在脚本中使用的各种内嵌对象。这些内嵌对象主要用于收集浏览器请求信息、响应浏览器和存储用户的各种信息，从而简化编程工作。ASP 结构提供 6 个内建对象：Request、Response、Application、Session、Server 和 ObjectContext。内建对象的特殊

性在于，它们在 ASP 页内生成且在脚本中使用它们前无须创建。

1)　Request 对象

Request 对象在 HTTP 请求期间，检索客户端浏览器传递给服务器的值。

其使用语法为

```
Request[.collection|property|method](variable)
```

Request 对象惟一的属性及说明如表 5-3 所示，它提供关于用户请求的字节数量的信息，很少用于 ASP 页，用户通常关注指定值而不是整个请求字符串。

表 5-3　Request 对象的属性及说明

属　性	说　明
Total Bytes	只读。返回由客户端发出的请求的整个字节数量

2)　Response 对象

Response 对象用来访问服务器端所创建的并发回客户端的响应信息。

其使用语法为

```
Response.collection|property|method
```

Response 对象也提供一系列的属性，可以读取和修改，使响应能够适应请求。这些由服务器设置，用户不需要设置它们。需要注意的是，当设置某些属性时，使用的语法可能与通常所使用的有一定差异。这些属性如表 5-4 所示。

表 5-4　Response 对象的属性及说明

属　性	说　明
Buffer-True|False	读写。布尔型。表明由一个 ASP 页所创建的输出是否一直存放在 IIS 缓冲区，直到当前页面的所有服务器脚本处理完毕或 Flush、End 方法被调用。在任何输出(包括 HTTP 报头信息)送往 IIS 之前，这个属性必须设置。因此在.}P 文件中，这个设置应该在<%@ LANGUAGE=...%>语句后面的第一行
CacheControl "setting"	读/写。字符型。设置这个属性为“Public”，允许代理服务器缓存页面，如为"Private"，则禁止代理服务器缓存的发生
Charest="value"	读/写。字符型。在由服务器为每个响应创建的 HTTP Content-Type 报头中附上所用的字符集名称
Content Type ="MIME-type"	读/写。字符型。指明响应的 HTTP 内容类型，标准的 MIME 类型(如 text/xml 或者 Image/gif)。假如省略，表示使用 MIME 类型 text/lhtml，内容类型告诉浏览器所期望内容的类
Expires minutes	读/写。数值型。指明页面有效的以分钟计算的时间长度，假如用户请求其有效期满之前的相同页面，将直接读取显示缓冲中的内容，这个有效期过后，页面将不再保留于私有(用户)或公用(代理服务器)缓冲中


续表

属　性	说　明
Expires Absolute#date[time]#	读写。日期/时间型。指明当一个页面过期和不再有效时的绝对日期和时间
Is Client Connected	只读。布尔型。返回客户是否仍然连接和下载页面的状态标志。在当前的页面已执行完毕之前，假如一个客户转移到另一个页面，这个标志可用来中止处理
PICS ("PIGS-Label-stringy")	只写。字符型。创建一个 PICS 报头并将之加到响应中的 HTTP 报头中，PICS 报头定义页面内容中的词汇等级，如暴力、性、不良语言等
Status="Code message"	读/写。字符型。指明发回客户的响应的 HTTP 报头中表明错误或页面处理是否成功的状态值和信息。例如“200 OK”和“404 Not Found”

3)　Application 对象

可以使用 Application 对象在给定的应用程序的所有用户之间共享信息。基于 ASP 的应用程序与所有的.asp 文件一样在一个虚拟目录及其子目录中定义。因为多个用户可以共享 Application 对象，所以必须有 Lock 和 Unlock 方法以确保多个用户无法同时更改某一属性。

其使用语法为

```
Application.method
```

Application 对象提供了在它启动和结束时触发的两个事件，如表 5-5 所示。

表 5-5　Application 对象的事件及说明

事　件	说　明
OnStart	当 ASP 启动时触发，在用户请求的网页执行之前以及任何用户创建 Session 对象之前。用于初始化变量、创建对象或运行其他代码
OnEnd	当 ASP 应用程序结束时触发。在最后一个用户会话已经结束并且该会话的 OnEnd 事件中的所有代码已经执行之后发生。其结束时，应用程序中存在的所有变量被取消

4)　Session 对象

可以使用 Session 对象存储特定用户会话所需的信息。这样，当用户在应用程序的 Web 页之间跳转时，存储在 Session 对象中的变量将不会丢失，而是在整个用户会话中一直存在下去。当用户请求来自应用程序的 Web 页时，如果该用户还没有会话，则 Web 服务器将自动创建一个 Session 对象。当会话过期或被放弃后，服务器将终止该会话。Session 对象最常见的一个用法就是存储用户的首选项。例如，如果用户指明不喜欢查看图形，就可以将该信息存储在 Session 对象中。

其使用语法为

```
Session.collection|property|method
```

Session 对象提供了 4 个属性，这些属性及说明如表 5-6 所示。

表 5-6　Session 对象的属性及说明

属　性	说　明
CodePage	读/写。整型。定义用于在浏览器中显示页内容的代码页(Code Page)。代码页是字符集的数字值，不同的语言和场所可能使用不同的代码页。例如，ANSI 代码页 1252 用于美国英语和大多数欧洲语言，代码页 932 用于日文字
LCID	读/写。整型。定义发送给浏览器的页面地区标识(LCID)。LCID 是惟一的标识地区的一个国际标准缩写，例如，2057 定义当前地区的货币符号是“£”。LCID 也可用于 FormatCurrency 等语句中，只要其中有一个可选的 LCID 参数。LCID 也可在 ASP 处理指令<%......%>中设置，并优先于会话的 LCID 属性中的设置，并优先于会话的 LCID 属性中的设置
Session ID	只读。长整型。返回这个会话的会话标识符，创建会话时，该标识符由服务器产生。在父 Application 对象的生存期内是惟一的，因此当一个新的应用程序启动时可重新使用
Timeout	读/写。整型。为这个会话定义以分钟为单位的超时周期。如果用户在超时周期内没有进行刷新或请求一个网页，该会话结束。在各网页中根据需要可以修改。默认值是 10min，在使用率高的站点上该时间应更短

5)　Server 对象

Server 对象提供对服务器上的方法和属性的访问。其中，大多数方法和属性是作为实用程序的功能服务的。

其使用语法为

```
Server.property|method
```

Server 对象的惟一一个属性用于访问一个正在执行的 ASP 网页的脚本超时值，如表 5-7 所示。

表 5-7　Server 对象的属性及说明

属　性	说　明
ScriptTimeout	整型。默认值为 90。设置或返回页面的脚本在服务器退出执行和报告一个错误之前可以执行的时间(秒数)。达到该值后将自动停止页面的执行，并从内存中删除包含可能进入死循环的错误的页面或者是那些长时间等待其他资源的网页。这会防止服务器因存在错误的页面而过载。对于运行时间较长的页面需要增大这个值

6)　ObjectContext 对象

可以使用 ObjectContext 对象提交或放弃一项由 Microsoft Transaction Server (MTS) 管理的事务，它由 ASP 页包含的脚本初始化。

当 ASP 页包含@TRANSACTION 指令时，该页会在事务中运行，直到事务成功或失败后才会终止。

其使用语法为

```
ObjectContext.method
```

5.2.1.2　JSP

JSP(Java Server Pages)是由 Sun Microsystems 公司倡导，许多公司共同参与建立的一种动态网页技术标准。在传统的网页 HTML 文件(*.htm、*.html)中加入 Java 程序片段(Scriptlet)和 JSP 标签，就构成了 JSP 网页(*.jsp)。Web 服务器在遇到访问 JSP 网页的请求时，首先执行其中的程序片段，然后将执行结果以 HTML 格式返回给客户。程序片段可以操作数据库、重新定向网页以及发送 E-mail 等，这就是建立动态网站所需要的功能。所有程序操作都在服务器端执行，网络上传送给客户端的仅仅是得到的结果，对客户端浏览器的要求最低，可以实现无 Plugin、无 ActiveX、无 Java Applet，甚至无 Frame。

1. JSP 的特点

与 ASP 和 PHP 相比，JSP 具有下列优点。

1)　内容的生成和显示分离

使用 JSP 技术，Web 页面开发人员可以使用 HTML 或者 XML 标签来设计和格式化最终页面。还可以使用 JSP 标签或者小脚本来生成页面上的动态内容。

2)　强调可重用的组件

绝大多数 JSP 页面依赖于可重用的、跨平台的组件(JavaBean 或 EJB)来执行应用程序所要求的更为复杂的处理。

3)　采用标识简化应用开发

通过开发定制化标识库，JSP 技术是可以扩展的。第三方开发人员和其他人员可以为常用功能创建自己的标识库。

4)　健壮性与安全性

由于 JSP 页面的内置脚本语言是基于 Java 编程语言的，而且所有的 JSP 页面都被译成 Java Servlet，所以 JSP 页面就具有 Java 技术的所有优点，包括健壮的存储管理和安全性。

5)　良好的移植性

作为 Java 的一部分，JSP 拥有 Java 编程语言“一次编写，各处运行”的特点。

6)　企业级的扩展性和性能

在与 Java 2 平台、J2EE 和 EJB 技术整合时，JSP 页面将提供企业级的扩展性和性能。

2. JSP 程序页面

下面是 JSP 的一个应用实例，主要完成日期对象的相关操作，首先获取系统当前时间，然后重新设置系统时间，将系统时间设置为北京 2008 年奥运会开始的时间。

```
<%@ page contentType="text/html; charset=GB2312" import = "java.util.*" %>
<HTML>
<HEAD>
<TITLE>日期对象各时间段的取得与设置</TITLE>
</HEAD>
<BODY>
<CENTER>
<FONT SIZE = 5 COLOR = BLUE>日期对象各时间段的取得与设置</FONT>
</CENTER>
```

```
<HR>
<P></P>
<%
//声明 Date 对象变量，并建立 Date 变量
Date date = new Date();
%>
当前系统日期为<Font color = red>
<%= date.getYear() + 1900%>/
<%= date.getMonth() + 1%>/
<%= date.getDate()%>
</Font><P></P>
当前系统时间为<Font color = red>
<%= date.getHours()%>:
<%= date.getMinutes()%>:
<%= date.getSeconds()%>
</Font><P></P>
<%
date.setYear(2008);      //将年设置为 2008 年
date.setMonth(8);        //将月设置为 8 月
date.setDate(8);         //将日设置为 8 日
date.setHours(8);        //将小时设置为 8 时
%>
重新设置的新时间为<Font color = red><%= date%></Font>是北京奥运会开始的时间。
</BODY>
</HTML>
```

该 JSP 页面经过 JSP 服务器解释在客户浏览器上显示的结果如图 5-4 所示。

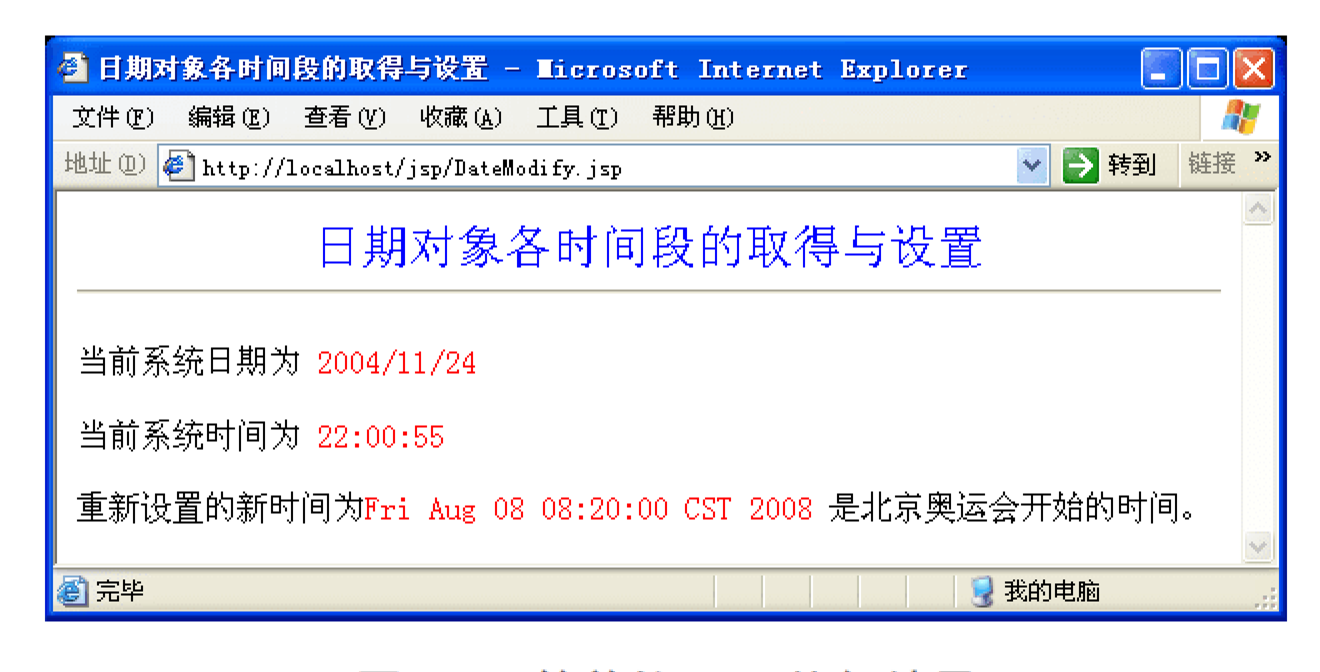


图 5-4　简单的 JSP 执行结果

3. JSP 技术的未来

JSP 技术被设计为一个开放的、可扩展的建立动态 Web 页面的标准。通过与业界领袖的合作，SUN 保证 JSP 规范的开放性和可移植性，可以使用任意客户机和服务器平台，在任何地方编写和部署它们。将来，工具供应商和其他厂商将通过为专门的功能提供客户化的标识库而扩展平台的功能。

5.2.1.3 PHP 和 ADO 数据库编程

1. PHP

PHP (Professional Hypertext Preprocessor)是一种服务器端 HTML 嵌入式脚本描述语言，目前正式发布的最高版本为 4.04。服务器端脚本技术又分为嵌入式与非嵌入式两种，PHP 是嵌入式的，类似的如 ASP。它是一种功能非常强大的、面向 Internet/Intranet 的编程语言，可以开发动态交互的 Web 应用程序，可在多种系统平台和多种 Web 服务器中使用，是真正的跨平台、跨服务器的开发语言。

PHP 语言的主要特征如下。

(1) 免费，轻巧快速，真正跨平台。

(2) PHP 是一种遵守 GNU 条约的软件。根据此条约，所有用户都可以免费使用 PHP 并可以得到它的源代码，还可以在源代码上进行修改和完善，开发成适合自己使用的新的版本。

(3) 易学易用。因为 PHP 3.0 以上版本是用 C 实现的，而且它自身的语法风格与 C 极其相似，有许多的语句、函数 PHP 与 C 是完全相同的。

(4) 具有十分强大的数据库操作功能，可直接连接多种数据库，并完全支持 ODBC。这一特点是其他脚本语言所不能比拟的。

(5) 可以嵌入 HTML 中。当使用者使用经典程序设计语言(如 C 或 Pascal 编程时，所有的代码必须编译成一个可执行的文件，然后该可执行文件在运行时，为远程的 Web 浏览器产生可显示的 HTML 标记。

2. ADO 数据库编程

微软公司的 ADO(ActiveX Data Objects)是一个用于存取数据源的 COM 组件。它是编程语言和统一数据访问方式 OLE DB 的一个中间层，允许开发人员编写访问数据的代码、到数据库的连接，而不用关心数据库的实现。ADO 的操作步骤如下。

(1) 打开连接。ADO 打开连接的主要方法是使用 Connection.Open 方法。另外，也可在同一个操作中调用快捷方法 Recordset.Open 打开连接并在该连接上发出命令。

(2) 创建命令。ADO 可提供简易灵活的方法，在单个步骤中创建 Parameter 对象并将其追加到 Parameter 集合。

```
cmd.Parameters.Append cmd.CreateParameter-
"au lname", adVarChar, adtnput, 40, "Ringer"
```

(3) 执行命令。返回 Recordset 的方法有三种：Connection.Execute、Command.Execute 和 Recordset.Open。以下是它们的 Visual Basic 语法：

```
connection.Execute(ConurtandText, RecordsAffected, Options)
command.Execute(RecordsAffected, Parameters, Options)
recordset.Open Source, ActiveConnection, CursorType,LockType,Options
```

(4) 操作数据。有多种方法可在 Recordset 中显式移动或“定位”(Move 方法)。一些方法(Find 方法)在其操作的附加效果中也能够做到。此外，设置某个属性(Bookmark 属性)同样可以更改行的位置。Filter 属性用于控制可访问的行(这些行是“可见的”)。Sort 属性用于

控制所定位的 Recordset 行中的顺序。Recordset 有一个 Fields 集合，它是在行中代表每个字段或列的 Field 集，可从 Field 对象的 Value 属性中为字段赋值或检索数据。作为选项，可访问大量字段数据(GetRows 和 Update 方法)。使用 Move 方法从头至尾对经过排序和筛选的 Recordset 进行定位。

(5) 更新数据。对于添加、删除和修改数据行，ADO 有两个基本概念。第一个是不立即更改 Recordset，而是将更改写入内部“复制缓冲区”；第二个是只要声明行的工作已经完成，则将更改立刻传播到数据源(“立即”模式)，或者只是收集对行集合的所有更改，直到声明该行集合的工作已经完成(“批”模式)。这些模式将由 CursorLocation 和 LockType 属性控制。

(6) 结束更新。ADO 检测到“冲突”并报告错误，如果错误存在，它们会被错误处理例程捕获。可使用 adFilterConflictingRecords 常数对 Recordset 进行筛选，将冲突行显示出来。要纠正错误只需打印作者的姓和名(au frame 和 au- lname)，然后回卷事务，放弃成功的更新。由此结束更新。

5.2.2　典型例题分析

例 1　阅读下列说明，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2009 年 11 月下午试题五)

【说明】

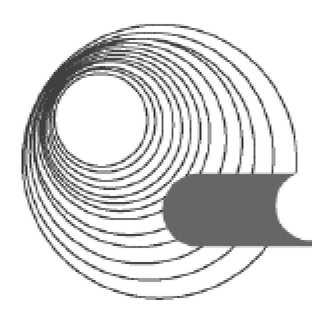
以下是用 ASP 实现的一个网上报名系统。用 IE 打开网页文件 index.asp 后的效果如图 5-5 所示。



图 5-5　网上报名系统显示效果

index.asp 文档的内容如下：

```
<%
set conn=server.CreateObject("adodb.connection")
conn.open"driver={MicrosoftAccessdiver(*.mdb)};dbq="&server.mappath("d
ate/date.mdb")
```




```
exec="select * from webset"
set rs=server.CreateObject("adodb.recordset")
rs. (1) exec,conn,1,1
%>
<head>
<title><%=rs("webname")%></title>
</head>

<html>
<img src="<%=rs ("logo")%>"alt=""winth="120" heigh="40" border="0"/>

<form action="register.asp" method="post" name="myform">
   <table width="100%" border="0" align="center" cellpadding="2"
cellspacing="1">
   <tr>
      <td colspan="4" align="left">注册信息</td>
   </tr>
   <tr>
      <td align="right" bgcolor="#FFFFFF">用户</td>
      <td colspan="3" bgcolor="#FFFFFF">
      <input type=" (2) " name="uname" value="<%=uname%>">
   </tr>
<tr>
   <td align="right" bgcoloi="#FFFFFF">密码</td>
   <td colspan="3" bgcolor="#FFFFFF"><input type="(3) " name="psd" ></td>
</tr>
<tr>
   <td colspan="4" align="left">报名信息</td>
</tr>
<tr>
   <td align="right" bgcolor="#FFFFFF">姓名</td>
   <td bgcolor="#FFFFFF"><input type="text" name="un" ></td>
</tr>
<tr>
   <td align="right" bgcolor="#FFFFFF">性别</td>
   <td bgcolor="#FFFFFF">
      <input type=" (4) " name="xb" value="male"/>男
      <input type=" (4) " name="xb" value=" female" checked=" true"/>女
   </td>
</tr>
<tr>
   <td align="right" bgcolor="#FFFFFF">电子邮箱</td>
   <td bgcolor="#FFFFFF"><input type="text" name="email" size="40"/></td>
</tr>
<tr>
   <td align="right" bgcolor="#FFFFFF">报考专业</td>
   <td bgcolor="#FFFFFF">
   <(5) name="zy">
      <option value="2000">计算机科学与技术</option>
```

```
        <option value="2001">电子工程</option>
        <option value="2002">通信工程</option>
    </select>
    </td>
</tr>
<tr>
    <td colspan="4" bgcolor="#FFFFFF">
        <input type="(6)"name="tijiao" value="提交">
    </td>
          </tr>
</table>
</form>
<tr><%=rs("copyright")%></tr>
<%
    rs.close()
%>
</html>
```

【问题 1】(2 分)

为程序中空缺处(1)选择正确答案。

A．Open　　B．Run　　C．Execute　　D．Dim

【问题 2】(10 分)

为程序中空缺处(2)～(6)选择正确答案。

A．Text　　B．Submit　　C．Password　　D．Radio

E．Checkbox　　F．Option　　G．Select　　H．Reset

【问题 3】(2 分)

该网页连接的数据库类型是<u>　(7)　</u>。

A．Oracle　　B．SQLServer　　C．Access　　D．DB2

【问题 4】(1 分)

HTML 文档中的<table>标记的 cellpadding 属性用于定义<u>　(8)　</u>。

备选答案：

A．内容对齐方式　　B．背景颜色

C．边线粗细　　D．单元格边距

分析：

【问题 1】

该语句表示打开数据集，故选 A。

【问题 2】

在 HTML 中，Text 标记为文本框，可以输入文字；Submit 标记为提交表单按钮；Password 为密码文本框；Radio 标记为单选按钮；Checkbox 标记为复选框；Select 标记为下拉列表框；Option 标记为下拉列表框中每一选项；Reset 标记为重置表单按钮标签，根据网页的显示，故选 A、C、D、G、B。

【问题 3】

conn.open"driver={Microsoft Access driver(*.mdb)};dbq=" &server. mappath("date/date.mdb"),

由该句可知其连接为 Access 数据库，故选 C。

【问题 4】

Html 中，<table>标记的 cellpadding 属性用于定义单元格边距，align 用于定义内容对齐方式，bgcolor 用于定义背景颜色，border 用于定义边线粗细。故选 D。

答案：

【问题 1】

(1) A

【问题 2】

(2) A

(3) C

(4) D

(5) G

(6) B

【问题 3】

(7) C

【问题 4】

(8) D

例 2 阅读以下说明，根据网页显示的效果图，回答问题 1～问题 3。(2009 年 5 月下午试题五)

【说明】

用 ASP 实现一个网上注册系统，用 IE 打开网页文件 index.asp 后的效果如图 5-6 所示。

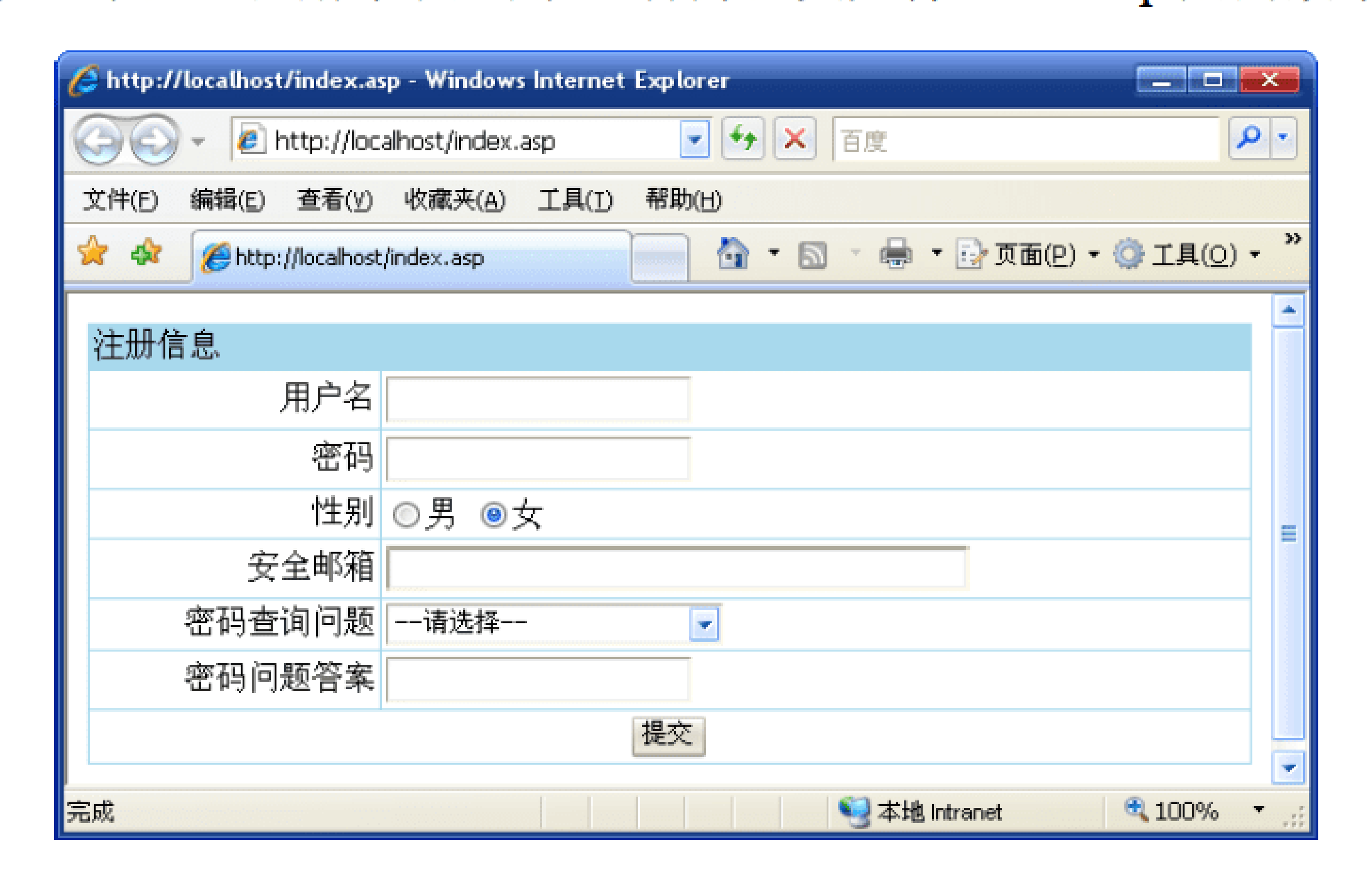


图 5-6 网上注册系统显示效果

index.asp 文档的内容如下：

```
<%
set conn=server.CreateObject("adodb.connection")
conn open"driver={Microsoft Access driver
("mdb")};dbq="&sever.mappath("date/date.mdb")
exec="select * from webset"
```

```
set rs=server.CreateObject("adodb.__(1)__")
rs.__(2)__exec,conn,1,1
%>
<head>
<title><%=rs("webname")%></title>
</head>
<html>

<form action="register.asp" method="post" name="myform">
<table  width="100%"  border="0"  align="center"  cellpadding="2"
cellspacing="1"  bgcolor="#A8D9EC">
  <tr>
    <td colspan="4" align="left">注册信息</td>
    </tr>
  <tr>
    <td  align="right"  bgcolor="#FFFFFF">用户名</td>
    <td colspan="3"  bgcolor="#FFFFFF">
      <input name="uname" type="__(3)__" value="<%=uname%>">
    </tr>
  <tr>
    <td align="right"  bgcolor="#FFFFFF">密码</td>
    <td colspan="3"  bgcolor="#FFFFFF"><input name="psd" type="__(4)__">
    </tr>

<tr>
    <td align="right"  bgcolor="#FFFFFF">性别</td>
    <td bgcolor="#FFFFFF">
      <input name="xb" type="__(5)__" value="male"/>男
      <input name="xb" type="__(5)__" value="female" checked="true"/>女
    </td>
  </tr>

  <tr>
    <td align="right"  bgcolor="#FFFFFF">安全邮箱</td>
    <td bgcolor="#FFFFFF"><input name="email" type="text" size="40"/></td>
  </tr>
  <tr>
  <td align="right"  bgcolor="#FFFFFF">密码查询问题</td>
  <td bgcolor="#FFFFFF">
  <__(6)__ name="zy">
    <option value="0">--请选择--</option>
    <option value="1">我小学校名是什么？</option>
    <option value="2">我最喜欢的歌曲是哪首？</option>
    <option value="3">我母亲的生日是哪天？</option>
    </select>
    </td>
  </tr>

  <tr>
```

```
      <td align="right"  bgcolor="#FFFFFF"密码问题答案</td>
      <td bgcolor="#FFFFFF"><input name="un" type="text"></td>
    </tr>
    <tr>
      <td colspan="4"  bgcolor="#FFFFFF">
      <input name="Submit" type="(7)  " value="提交">
    </td>
    </tr>
  </table>
  </form>

  <tr><%=rs("copyright")%></tr>
  <%
     rs.close()
  %>

  </html>
```

【问题 1】(4 分)

从以下备选答案内为程序中(1)～(2)处空缺选择正确答案，并填入答题纸对应的解答栏内。

(1) A. connection　　B. stream　　C. recordset　　D. command

(2) A. Open　　B. Run　　C. Execute　　D. Dim

【问题 2】(每空 2 分，共 10 分)

从以下备选答案内为程序中(3)～(7)处空缺选择正确答案，并填入答题纸对应的解答栏内。

A. Text　　B. Submit　　C. Password　　D. Radio

E. Checkbox　　F. Option　　G. Select　　H. Reset

【问题 3】(1 分)

HTML 文档中<table>标记的 cellpadding 属性用于定义 (8) 。

A. 内容对齐方式　　B. 背景颜色　　C. 边线粗细　　D. 单元格边距

分析：

【问题 1】本题主要考查通过 ADO 访问数据库的方法。

通过调用 Server 对象的 CreateObject 方法创建一个 Connection 接口，具体命令为 server.CreateObject("adodb.connection")。

然后使用 Connection 对象的 Open 方法来初始化连接，只有使用了 Connection 对象的 Open 方法之后，Connection 对象才会真正存在，然后才能发出命令对数据源产生作用。

Connection 对象处理数据时，常常要创建一个 RecordSet，RecordSet 允许用户对数据提供者进行访问。通过使用 RecordSet 对象，可以很方便地从数据库中读取数据，还可以向数据库增加数据。创建 RecordSet 对象的方法为：Server.CreateObject("adodb.RecordSet")。

创建了一个 RecordSet 对象之后，可利用其 Open 方法和数据表 exec 建立连接，这样就可以对数据表进行操作了。

【问题 2】主要考查超文本标记语言 HTML，特别是表单。由图 5-6 可知，【用户名】

后是普通的文本框，输入的文本以标准的字符显示，因此 type 属性为 text。【密码】后面为特殊的文本框，输入的文本显示为“*”，因此 type 属性应为 password。【性别】处为单选按钮，一次只能选中一个选项，type 属性应为 radio。【密码查询问题】处为下拉列表，要通过 select 标记来实现。【提交】按钮用于将表单内容传送给 action 中的网址，其 type 属性为 submit。

【问题 3】cellpadding 用于定义表项内部空白，即单元格边距，单位是像素。设置内容对其方式的属性是 align。定义背景颜色的属性是 bgcolor。定义边线粗细的属性是 border。

答案：

【问题 1】(1) C　(2) A

【问题 2】(3) A　(4) C　(5) D　(6) G　(7) B

【问题 3】(8) D

例 3　阅读下列说明，根据网页显示的效果图，回答问题 1～问题 4。(2008 年 11 月下午试题五)

【说明】

以下是用 ASP 实现的一个网络论坛系统，用 IE 打开网页文件 index.asp 后的效果如图 5-7 所示。

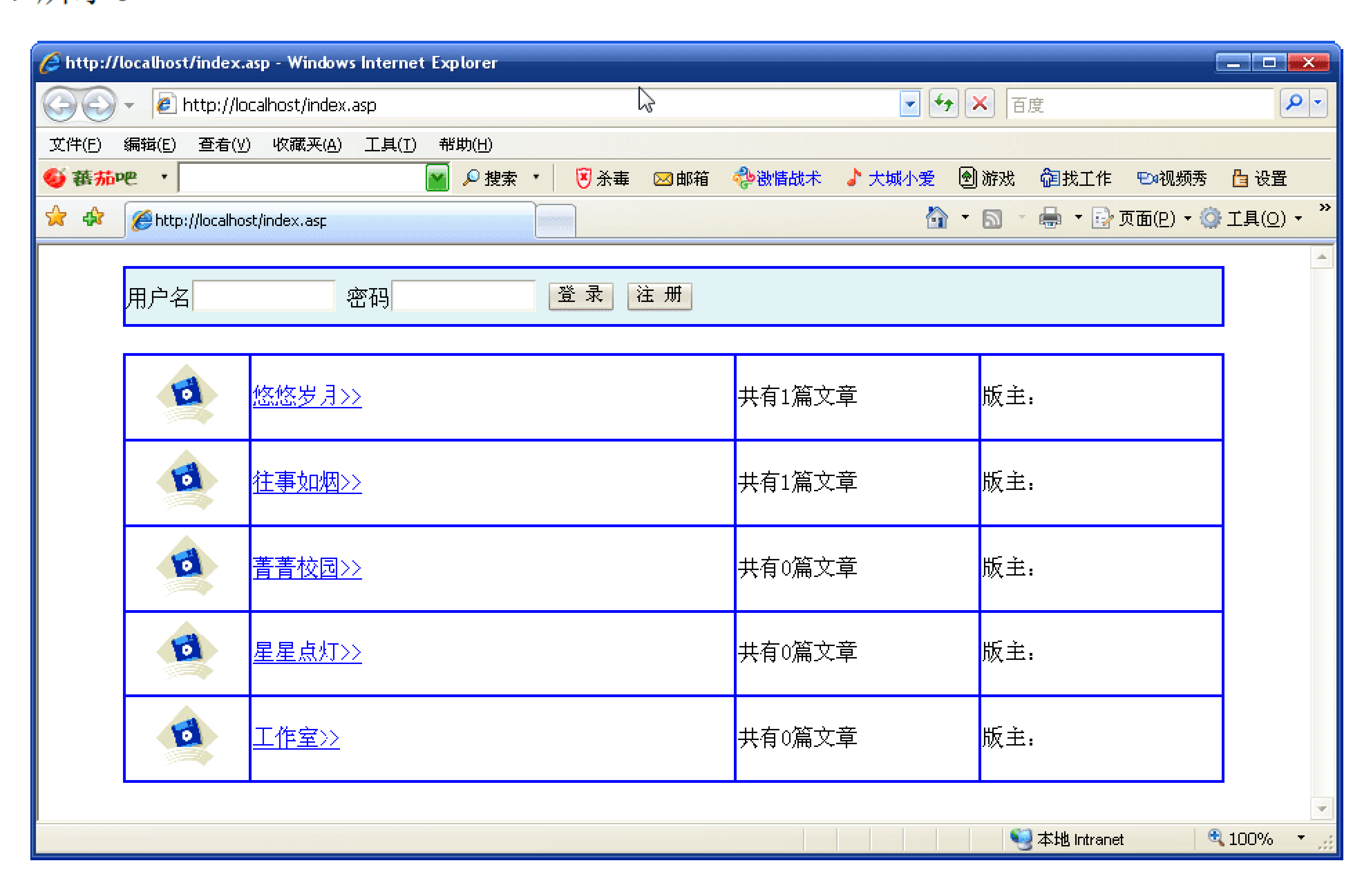
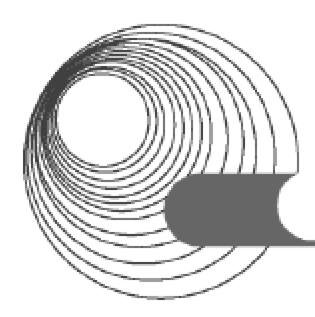


图 5-7　网络论坛系统显示效果

index.asp 文档的内容如下：

```
<%
set db=server.createobject("Adodb.Connection")
db.___(1)___ "Dbq="& server.mappath("data/bbs.mdb") & "; Driver={Microsoft
Access Driver(*.mdb)}"
%>
<html>
```




```
<body>
<form name="form1" method="post" action="aaa.asp">
  <table border="0" bgcolor="#0000FF" width="800" cellpadding="0"
align="center">
<tr>
    <img src="images/logo.gif" width="190" height="94">
</tr>
<tr bgcolor="#E1F3F4" height="40">
<td>
    用户名<input type="text" name="user_id" size=13 class="input">
    密码< input type="PassWord" name="password" size=13 class="input">
<input class="inputbutton" type="submit" value="登 录" name="Submit">
<input class="inputbutton" onClick="window.open('bbb.asp', '_self')"
type="button" value="注 册" name="register">
    </td>
  </tr>
  </table>
 </form>
<table border="0" bgcolor="#0000FF" width="800" align="center">
<%
'打开记录集，显示所有论坛栏目
dim rs,strSql
strSql="select * from forum"
set rs=db.___(2)___(strSql)
Dim no                          '该变量用来显示图片
no=0
do while Not ___(3)___
no=no+1
%>
<tr bgcolor="#E1F3F4" height="60" valign="middle">
<td width="10%" align="center" bgcolor="#FFFFFF">
     <a href="ccc.asp?forum_id=<%=rs("ID")%>"><img src="images/<%=no%>.gif
border="0"></a>
</td>
<td width="40%" align="left" bgcolor="#FFFFFF">
     <a
href="ddd.asp?forum_id=<%=rs("ID")%>"><%=rs("forumname")%>&gt;&gt;</a>
</td>
<td width="20%" align="left" bgcolor="#FFFFFF">共有<%=rs("forumcount")%>篇
文章
</td>
<td width="20%" bgcolor="#FFFFFF">版主
        <%=rs("manager")%>
</td>
</tr>
<%
     rs.___(4)___
     loop
     '关闭对象
```

```
        db.Close
        Set db=Nothing
      %>
    </table>
    </body>
    </html>
```

【问题 1】(每空 2 分，共 8 分)

从以下备选答案内为程序中(1)～(4)处空缺选择正确答案，并填入答题纸对应的解答栏内。

(1)　A. open　　B. run　　C. execute　　D. Dim

(2)　A. open　　B. run　　C. execute　　D. Dim

(3)　A. db. Bof　　B. db. Eof　　C. rs. Bof　　D. rs. Eof

(4)　A. go　　B. movenext　　C. skip　　D. next

【问题 2】(2 分)

HTML 文档中的<table>标记的 cellpadding 属性用于定义__(5)__。

A. 内容对齐方式　　B. 背景颜色　　C. 边线粗细　　D. 单元格边距

【问题 3】(3 分)

单击网页中的【登录】按钮，将会执行的程序为__(6)__。

A. aaa. asp　　B. bbb. asp　　C. ccc. asp　　D. ddd. asp

【问题 4】(2 分)

该网页连接的后台数据库类型是__(7)__。

A. Oracle　　B. SQLServer　　C. Access　　D. DB2

分析：

【问题 1】

本题是考查 ASP 动态网页编程技术中的一些命令。

首先声明了一个 db 的变量，将变量 db 初始化为一个 ADODB.Connection 对象，然后调用这个对象的 open 方法，用来打开一个连接。

Connection 对象 db 也能执行 SQL 语句及存储过程，需要用到 execute 方法。利用该对象来返回数据时，要抽取的信息是基本的游标，即只能读和只能向前的游标。使用 rs.movenext()可把指针向下移动，但不能无限制地移动，如果到了记录集的最后还使用此方法，就会产生错误。可用 RecordSet.Eof 判断是否到达最后。游标的 bof 和 eof 属性是用来判断是否到达 RecordSet 的首记录和尾记录。rs.eof=true 时表明指针已移到尾记录。

【问题 2】

表格使用 table 元素定义。tr 用来定义表行，th 用来定义表头，td 用来定义表格数据。

单元格间隙可以通过 cellspacing 来定义，边线粗细可使用 border 属性来定义：<table border=n width=x height=y cellspacing=i cellpadding=j>。

内容对齐方式可使用 align 属性来定义，可在<col>、<colgroup>、<th>、<td>、<tr>标记中使用 align 属性设置表项数据的水平对齐方式，使用 valign 属性设置垂直对齐方式。

背景颜色可使用 bgcolor 属性来定义，可在<table>、<th>、<tr>、<td>标记中使用 bgcolor

属性。

【问题 3】

单击网页中的【登录】按钮，会将表单内容传送到 action 中指定的程序并执行，该程序为 aaa.asp。

【问题 4】

Driver={Microsoft Access Driver (*.mdb)}表明该网页连接的后台数据库类型是 Access。

答案：

【问题 1】(1) A　(2) C　(3) D　(4) B

【问题 2】(5) D

【问题 3】(6) A

【问题 4】(7) C

例 4　阅读以下说明，根据网页显示的效果图，回答问题 1～问题 4，将解答填入答题纸对应的解答栏内。(2008 年 5 月下午试题五)

【说明】

以下是用 ASP 实现的一个在线留言系统，用 IE 打开网页文件 index.html 后的效果如图 5-8 所示。

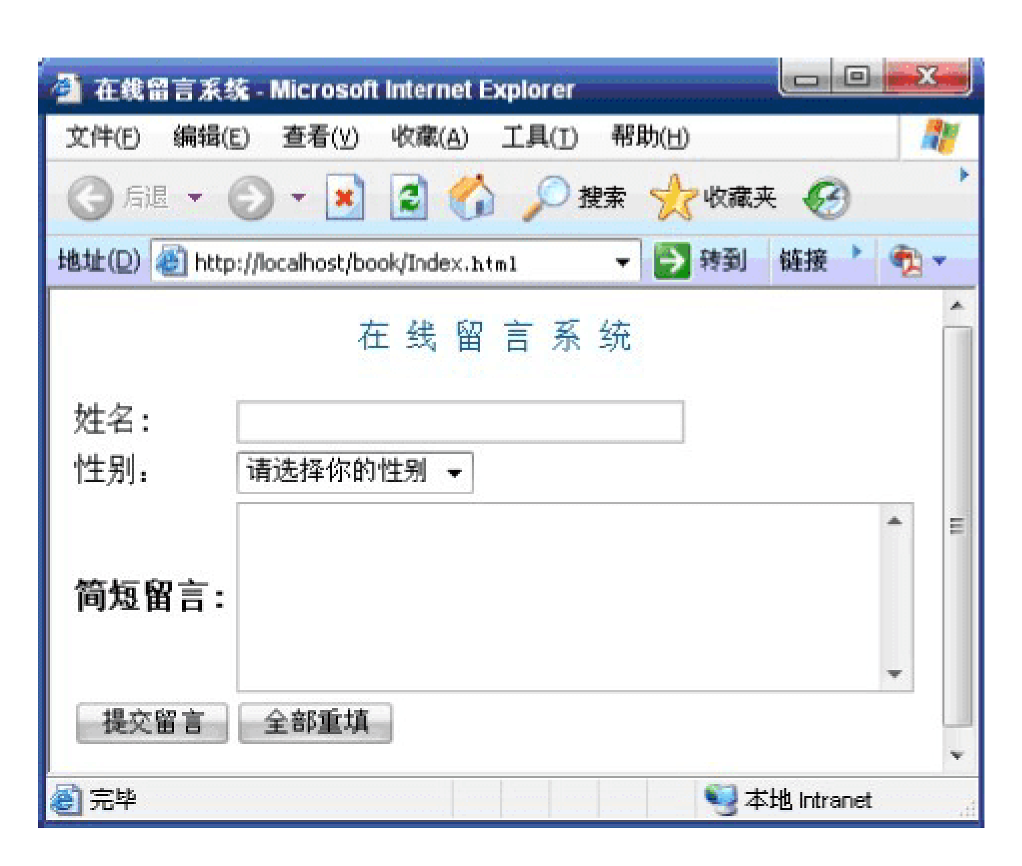


图 5-8　在线留言系统显示效果

index.html 文档的内容如下：

```
<html>
<head>
<title>在线留言系统</title>
</head>
<body>
<p align="center"><font color="#006699">在线留言系统</font></p>
<form method="post" action="submit.asp">
<table border="0" cellspacing="1" width="89%">
<tr>
<td>姓名：</td>
<td><__(2)__name="name" size="30" class="text"maxlength="20"></td>
</tr>
```

```
<tr>
<td>性别：</td>
<td><__(3)__name="sex" size="1"
<option selected>请选择你的性别</option>
   <option value="男">男</option>
   <option value="女">女</option>
   </select></td>
</tr>
<tr>
<td><b>简短留言： </b></td>
<td><__(4)__name="content" rows="6" cols="45" class="tsxt"></textarea></td>
</tr>
<tr>
<td><__(5)__name="submit" class="btn" value="提交留言"></td>
<td><__(6)__name=:B1" value="全部重填" class="btn"></td>
</tr>
</table>
</form>
</body>
</html>
```

submit.asp 文档的内容如下：

```
<%
If request.form("name")="" Then
  response.write"<script>alert('请填写留言人姓名！';history.back()</script>"
response.end
End If
If request.form("sex")='" or request.form("sex")="请选择你的性别" Then
  request.write"<script>alert('请选择留言人性别'); history.back()</script>"
  response.end
End If
If len(__(7)__)>100 Then
request.write"<script>alert('留言不能超过 100 字!');history.back()</script>"
response.end
End If
%>
<!--#include file="conn.asp"-->
<%
dim rs,sql
set rs=server.__(8)__
sql="select * from data where ( id is null)"
rs.open sql,conn,1,3
rs.__(9)__
rs("name")=__(10)__
rs("sex")=request.form("sex")
rs("content")= request.form("content")
rs("date")=now()
rs("ip")=request.ServerVariables("remote_addr")
```

```
rs.  (11)  
rs.close
conn.close
response.redirect "success.asp"
%>
```

【问题 1】(2 分)

将以上 index.html 更名为 (1) 后，将不能直接在 IE 中正常显示该网页。

A. index.html　　B. index.php　　C. index.asp

【问题 2】(5 分)

为 index.html 文件中的(2)～(6)处空缺选择正确答案。

A. input type="reset"　　B. input type="submit"　　C. input type="text"

D. textarea　　E. option　　F. select　　G. radio

【问题 3】(5 分)

从以下备选答案中为 submit.asp 程序中(7)～(11)处空缺选择正确答案。

(7) A. request.querystring("content")　　B. request.querystring("name")

C. request.form("content")　　D. request.form("name")

(8) A. mappath("adodb.recordset")　　B. createobject("adodb.recordset")

C. new("adodb.recordset")　　D. htmlencode("adodb.recordset")

(9) A. addnew　　B. add

C. eof　　D. insert

(10) A. request.querystring("content")　　B. request.querystring("name")

C. request.form("content")　　D. request.form("name")

(11) A. submit　　B. update　　C. append　　D. refresh

【问题 4】(3 分)

response.redirect "success.asp"语句的作用是 (12) 。

A. 弹出 success.asp 网页窗口

B. 重定向到 success.asp 网页

C. 关闭 success.asp 程序

D. 修改 success.asp 程序

分析：

【问题 1】

IE 可以正常解析后缀为.html 和.htm 的网页文件。同时，如果文件的后缀名为.asp，那么 IE 在得到服务器对 ASP 文件的处理所得的 HTML 代码后，也可正常显示。本题中将普通.html 文件改名为以.asp 为后缀，显然其中不含 ASP 程序，因此 IE 可正常显示。而 IE 无法显示后缀为.php 的文件。

【问题 2】

本题主要考查表单操作。由图 5-8 可知，【姓名】后是普通的文本框，完整的标记语句为<input type=text name="name" size="30" class="text" maxlength="20">。【性别】处为下拉列表，要通过 select 标记来实现。【简短留言】后为文本区域，通过 textarea 标记实现。【提交留言】按钮用于将表单内容传送给 action 中的网址，完整的标记语句为：< input

type="submit" name="submit" class="btn" value="提交留言">。【全部重填】按钮可将表单内容全部清除，重新输入数据，完整的标记语句为<input type="reset" name=:B1" value="全部重填" class="btn">。

【问题 3】本题主要考查通过 ADO 访问数据库的方法。

request 提供了 5 个集合，用来访问客户端对 Web 服务器请求的各种信息。当用户在表单中使用 Get 方法传输数据时，用户提交的数据不是被当作一个单独的包发送，而是被附加在查询字符串中，服务器端可用 QueryString 组件从查询字符串中读取用户提交的数据。当用 post 方法将表单提交给服务器时，ASP 的 Request 对象特别指定了一个 Form 集合来进行相关处理。本题中使用的是 post 方法，因此要采用 Form 集合对留言区域进行处理，获取数据的方法是：request.form("content")。

ADO 中的 Connection 对象是一个开放连接，它跟踪正在使用的数据源。创建一个 Connection 接口需要调用 Server 对象的 CreateObject 方法：server.CreateObject ("adodb.connection")。

Connection 对象调用 Open 方法来初始化与数据库的连接，语法为

```
Connection.Open [ConnectionString],[UserID],[Password],[Options]
```

在客户端，用户提交了留言信息后，通过 RecordSet 的 AddNew 方法把该信息作为一条记录添加到数据库中。调用该方法时在 RecordSet 中开始一个新行，并将指针移到行首准备加入新数据。通过以下命令将用户名、性别、留言、留言发表时间、客户机 IP 地址添加到记录中。

```
rs("name")= request.form("name")
rs("sex")=request.form("sex")
rs("content")= request.form("content")
rs("date")=now()
rs("ip")=request.ServerVariables("remote_addr")
```

添加记录后，通过 update 方法将对 RecordSet 对象中的当前记录的任何修改保存到数据库中。

【问题 4】

response.redirect 语句的作用是使浏览器重新定位到另一个 URL 上，完成页面转换。response.redirect "success.asp"语句的作用是重定向到 success.asp 网页。

答案：

【问题 1】

(1) B

【问题 2】

(2) C　(3) F　(4) D　(5) B　(6) A

【问题 3】

(7) C　(8) B　(9) A　(10) D　(11) B

【问题 4】

(12) B

例 5　阅读下列说明，根据网页显示的效果图，回答问题 1～问题 6。(2007 年 11 月下午试题五)

【说明】

以下是用 ASP 实现的一个网络留言系统，用 IE 打开网页文件 index.asp 后的效果如图 5-9 所示。

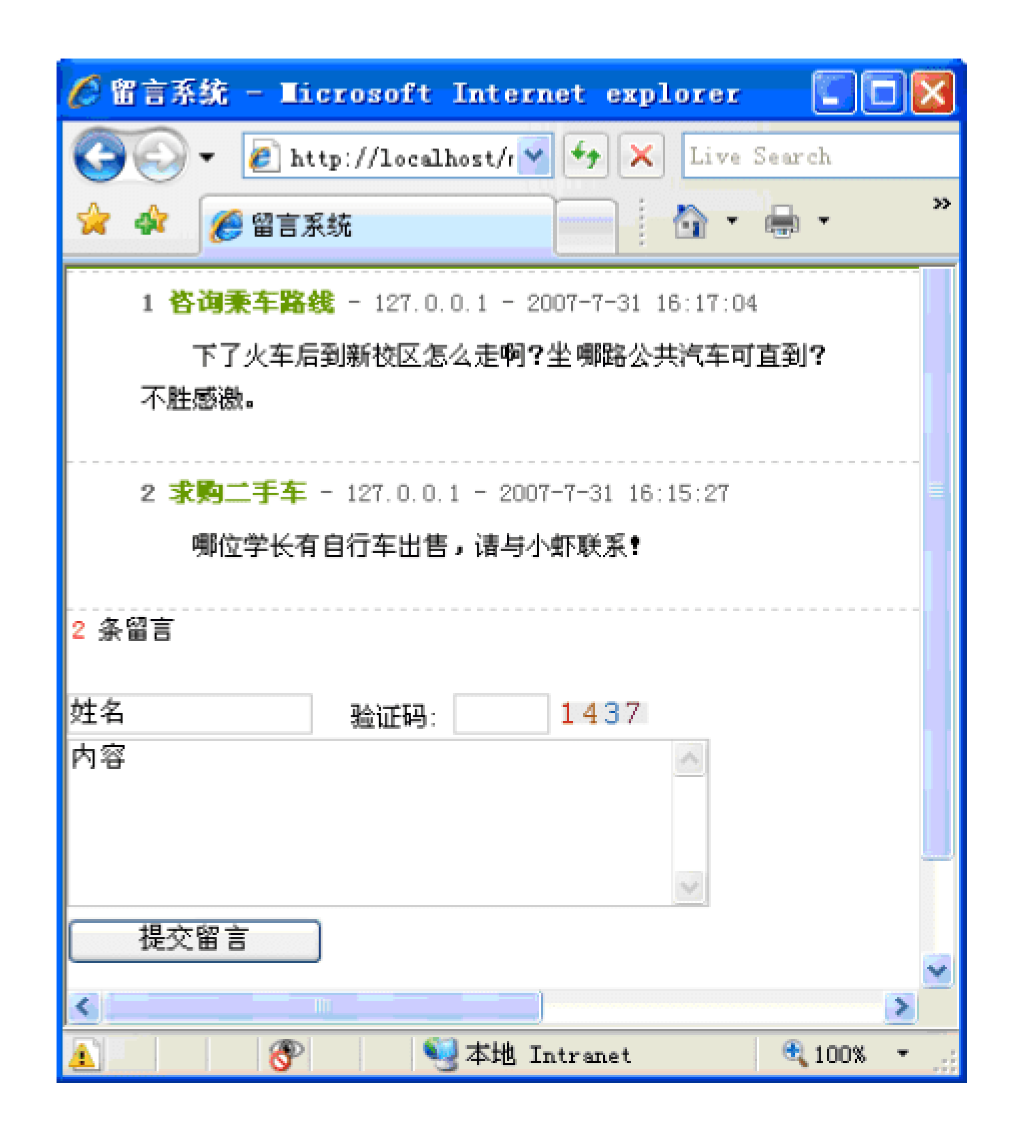


图 5-9　网络留言系统显示效果

index.asp 文档的内容如下：

```
<!--#include file="conn.asp"-->
<html>
<head><title>留言系统</title></head>
<body>
<%Set rs = Server.CreateObject("ADODB.Recordset")
rs.Open "Select * From [message] order by id",Conn,1,1
if rs.eof and rs.bof then
   ___(3)___.write("<div align='center' class='bg'>没有留言</div>")
end if
i=1
do while ___(4)___
%>
<table width="700" border="1" align="center" >
  <tr>
    <td height="30"><strong><%= ___(5)___%></strong>
        <%=rs("name")%> <%=rs("ip")%> <%=rs("time")%>
        <a href="del.asp?del=<%=rs("id")%>" target="_parent">删除</a>
    </td>
  </tr>
  <tr>
    <td width="700" height="20"><%=rs("message")%></td>
  </tr>
</table>
```

```
<%rs.movenext
i=i+1
loop
%>
<table width="700" border="0" align="center">
  <tr>
    <td><div align="left"><%=rs. recordcount%>条留言</div></td>
  </tr>
</table>
<br />
<table width="704" border="0" align="center">
  <tr>
    <td width="311"><form id="form1" name="form1" method="post"
action="act.asp">
      <table width="302" border="0">
        <tr>
          <td width="302">姓名<input name="name" type="text" class="box"
id="name" size="15" /><p/>
          验证码<input name='validatecode' type='text' class="box" size='5'>
          <img src='imgchk/validatecode.asp' align='absmiddle'
border='0'> </td>
        </tr>
        <tr>
          <td>内容 (6) </td>
        </tr>
        <tr>
          <td height="30"><input type=" (7) " name="tj" value="  提交留言  " />
            <input name="ip" type="hidden" id="ip" value= "<%=
Request.serverVariables("REMOTE_ADDR")%>" /></td>
        </tr>
      </table>
    </form>
 </td>
  </tr>
</table>
<%rs.close %>
</body>
</html>
```

【问题 1】(2 分)

以下 (1) 属于 ASP.NET 创建的网页程序文件。

A. index.asp　　B. index.htm　　C. index.aspx

【问题 2】(2 分)

HTML 文档中的<title>标签用于定义 (2) 。

A. 修改标记　　B. 显示标题　　C. 元数据

【问题 3】(每空 1 分，共 5 分)

从以下备选答案内为程序中(3)～(7)处空缺选择正确答案，并填入答题纸对应的解答

栏内。

(3) A. request　B. response　C. application　D. session

(4) A. rs.eof　B. rs.bof　C. not rs.eof　D. not rs.bof

(5) A. i+1　B. rs.recordnumber
C. rs.recordcount　D. i

(6) A. <table name="message" cols="40" rows="5" id="message"></table>
B. <textarea name="message" cols="40" rows="5" id="message"></textarea>
C. <input name="message" cols="40" rows="5" id="message"></input>
D. <img name="message" cols="40" rows="5" id="message"></img>

(7) A. submit　B. text　C. post　D. radio

【问题 4】(2 分)

另一个与程序中的语句 rs.eof and rs.bof 等价的语句是__(8)__。

【问题 5】(2 分)

设置验证码的作用是__(9)__。

【问题 6】(2 分)

rs.close 语句的作用是__(10)__。

A. 关闭数据库连接　B. 关闭当前网页
C. 关闭当前数据集　D. 关闭数据提交

分析：

【问题 1】

本题考查 ASP.NET 动态网页技术。

ASP.NET 是继 ASP 后推出的新一代动态网页编程环境，其网页程序文件名的后缀应该是.aspx 的形式。

【问题 2】

本题考查 HTML 标记的作用。

<title>和</title>标记中间所包含的文字，就是这个 Web 页面的标题，它写在头部标记之中。标题会显示在 Web 浏览器最上面的 title(标题)栏的位置。用户可以把标题加入 Bookmark(书签)中，还可以提供加入 Hostlist 或 Bookmark 列表的文本，所以一定要使<title>文本有明确的意义，其语法格式一般为

```
<title>Web 页面的标题</title>
```

【问题 3】

本题考查 HTML 和 ASP 编程的语法知识。

Active Server Pages 提供内建对象，这些对象使用户更容易收集通过浏览器请求发送的信息、响应浏览器及存储用户信息。以下简要说明每一个对象。

Application 对象：用于在给定应用程序的所有用户之间共享信息。

Request 对象：使用 Request 对象访问任何用 HTTP 请求传递的信息，包括从 HTML 表格用 POST 方法或 GET 方法传递的参数、Cookie 和用户认证。Request 对象使用户能够访问发送给服务器的二进制数据，如上传的文件。

Response 对象：用于控制发送给用户的信息。包括直接发送信息给浏览器、重定向浏览器到另一个 URL 或设置 Cookie 的值。

Server 对象：提供对服务器上的方法和属性进行的访问。最常用的方法是创建 ActiveX 组件的实例(Server.CreateObject)。其他方法用于将 URL 或 HTML 编码成字符串，将虚拟路径映射到物理路径及设置脚本的超时期限。

Session 对象：用于存储特定的用户会话所需的信息。当用户在应用程序的页之间跳转时，存储在 Session 对象中的变量不会清除；而用户在应用程序中访问页时，这些变量始终存在。也可以使用 Session 方法显式地结束一个会话和设置空闲会话的超时期限。

ObjectContext 对象：用于提交或撤销由 ASP 脚本初始化的事务。

【问题 4】

本题考查数据集记录为空的判定语句。

语句 rs.eof and rs.bof 如果为真，表示当前数据集中的记录为 0。同时，可以使用数据集 rs 的另一个属性 recordcount 来完成同样的功能。

【问题 5】

本题考查在 Web 网页中设置验证码的作用。

验证码可以有效地阻止 HTML 页面提交的穷举法。穷举法就是利用一些字母组合来不断尝试，直到找到正确的密码。在尝试的过程中，真正的密码一般要不变，如果真正的密码不断改变就大大增加了破解的难度，几乎就不可能破解成功。验证码正是利用了穷举法的这一弱点，在验证时加入动态的验证内容，有效地防止了穷举法的攻击。

验证码在 Web 服务器上随机产生并自己记录下来，再生成文字传给用户。用户照着手动输入提交，服务器对提交的验证码与记下来的验证码进行比较，如果都正确而且用户名也正确就通过验证。

【问题 6】

本题考查动态网页中数据库连接方面的知识。

在 ASP 中连接 Access 数据库常用 Access OLE DB 连接方法。具体步骤为：

```
strconn = "DRIVER=Microsoft Access Driver (*.mdb);DBQ=" & Server.MapPath
("aspfree.mdb")
set conn = server.createobject("adodb.connection")
conn.open strconn
```

而关闭数据集使用语句 rs.close。

答案：

【问题 1】

(1) C

【问题 2】

(2) B

【问题 3】

(3) B　(4) C　(5) D　(6) B　(7) A

【问题 4】

(8) rs.recordcount=0

【问题 5】

(9) 验证码能够有效地防止用特定程序不断进行登录尝试，破解其他用户的帐号和密码。

【问题 6】

(10)C

例 6　阅读下列说明，根据网页显示的效果图，回答问题 1～问题 7。(2007 年 5 月下午试题五)

【说明】

以下是用 ASP 实现了一个网络收藏夹网页，用于保存用户感兴趣的 Web 网页地址。用 IE 打开网页 index.asp 后的效果如图 5-10 所示。程序中使用的数据表 address 结构如表 5-8 所示。

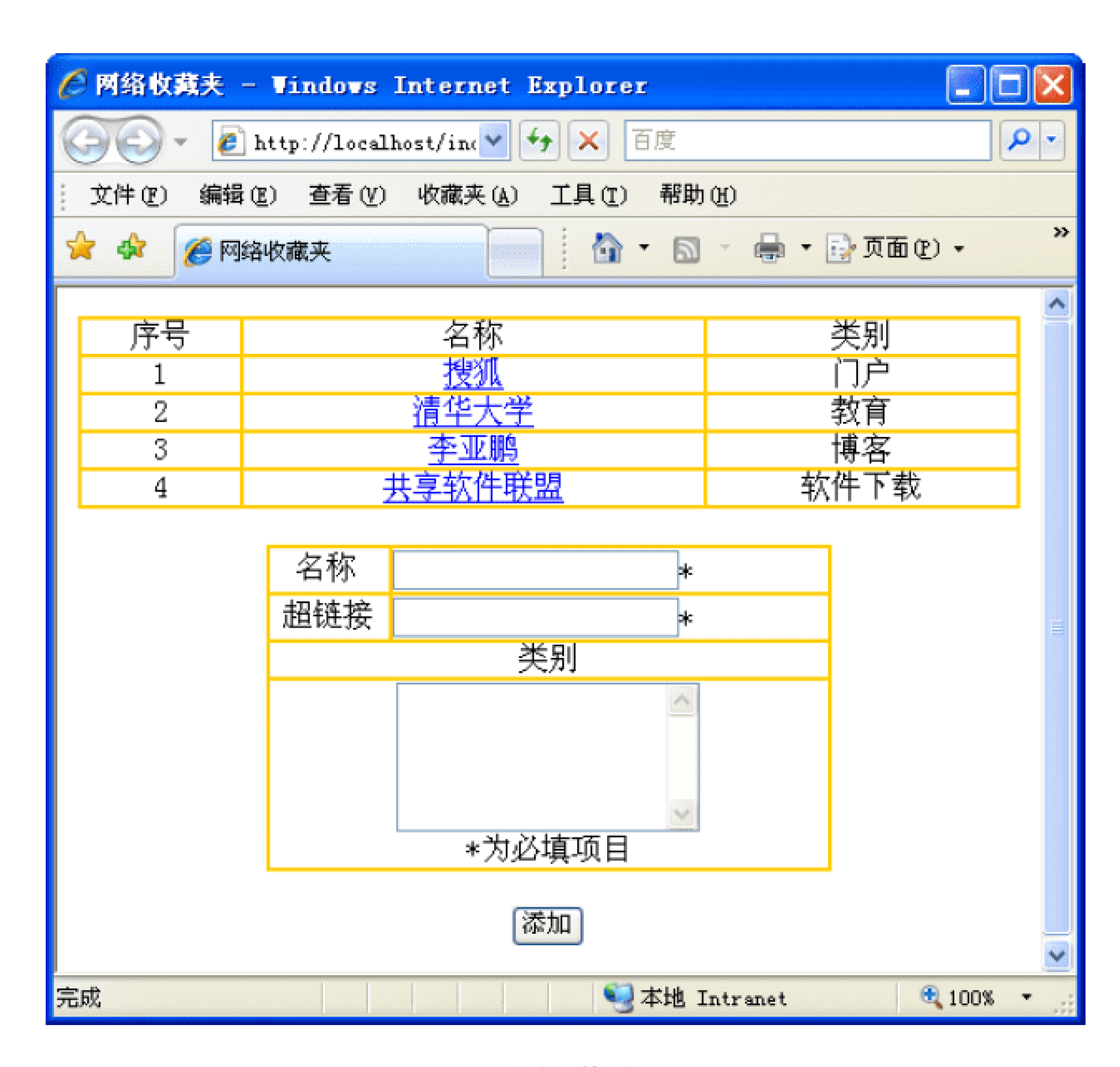


图 5-10　网络收藏夹网页界面图

表 5-8　address 数据表结构

字 段 名	类　型	备　注
no	自动编号	序号
name	文本	主页名称
url	文本	超链接
category	文本	网站类别

indet.asp 文档的内容如下：

```
<%@LANGUAGE="VBSCRIPT"%>
<%
 set conn=server.__(5)__("Adodb Connection")
 provider="Provider=Microsoft.Jet.OLEDB.4.0;"
```

```
 path="Date Source=" & Server.MapPath("main.mdb")
 connstr=provider & path
 conn.open connstr
%>
<html>
<head><title>网络收藏夹</title></head>
 (6) 
<center>
<%
    set rs=Server.CreateObject("Adodb.RecordSet")
    sql="select*from address"
    rs open()sql,conn,1,3
 if Request("name")=""or Request("url")=""then
        Response.write("内容填写不完整")
 else
   rs.addnew
   rs(1)=request("name")
   rs(2)=request("URL")
   rs(3)=request("category")
   rs.update
 end If
%>
<table width="500" border="1" cellpadding="0" cellspacing="0"
bordercolor="#FFCC00">
<tr><td>序号</td><td>名称</td><td>类别</td></tr>
<%rs.movefirst
for j=1 to rs. (7) %>
  <tr>
  <td><%=j%></td>
  <td><a href="<%=rs("url")%>"targer="blank"><%"rs("name")%></a></td>
  <td><%=rs("category")%></td>
      </tr>
<%rs.movenext
  (8) %>
</table><br>
<form action="index.asp" method="post" name="new" id="new">
  <table width="300" border="1" cellpadding="0" cellspacing="0"
bordercolor="#FFCC00">
    <tr>
      <td width="61">名称</th>
      <td width="223" align="left"><input name="neme" type="text"
id="name"></td>
    </tr>
    <tr>
      <td>超链接</td>
      <td width="left"><input name="URL" type="text" id="URL"></td>
    </tr>
    <tr>
      <td colspan="2">类别</td>
```

```
    </tr>
    <tr>
      <td colspan="2"><textarea name="category" rows="5"
id="disc"></textarea>
        <br>*为必填项目</td>
      </tr>
</table>
<br>
 (9) 
</forn>
<%
rs close
conn.close
%>
</center>
</body>
</html>
```

【问题 1】(2 分)

ASP 是 (1) 网页制作技术。

A. 动态　　B. 静态

【问题 2】(2 分)

(2) 是矢量动态工具。

A. flash　　B. jpg　　C. bmp

【问题 3】(2 分)

以下文件中 (3) 属于动态网页文件。

A. index/htm　　B. index. asp　　C. index. html　　D. index. exe

【问题 4】(2 分)

三层 B/S 结构中包括浏览器、服务器和 (4) 。

A. 解释图　　B. 文件系统　　C. 缓存　　D. 数据库

【问题 5】(每空 1 分，共 5 分)

从以下备选答案内为程序中(5)～(9)处空缺部分选择正确答案，并填入答题纸对应的解答栏内。

(5) A. CreatObject　　B. Connect　　C. ExecuteSQL　　D. Open()

(6) A. <body>　　B. <html>　　C. <head>　　D. <table>

(7) A. number　　B. recordnumber　　C. count　　D. recordcount

(8) A. skip　　B. end for　　C. next　　D. loop

(9) A. <input type="submit" name="add" value="添加">

B. <input type="post" name="add" value="添加">

C. <input type="submit" name="添加" value="add">

D. <input type="post" name="添加" value="add">

【问题 6】(1 分)

网页中使用的数据库连接引擎是什么？连接的后台数据库文件名是什么？

【问题 7】(1 分)

假设连接的数据记录当前指向的记录如下。

no	name	url	category
5	百度	http://www.baidu.com	搜索引擎

写出以下 ASP 代码经过 IIS 服务器解释后的结果。

```
<a href="<%=rs("url")%>"target="_blank"><%=rs("name")%></a>
```

分析：

【问题 1】

本题考查的是 ASP 技术的特点。

ASP 是一种动态网页技术，这是它不同于一般静态网页技术如 JavaScript 等的根本特点。动态网页技术是指浏览器最终显示的网页是在 Web 服务器上动态产生的，而不是事先就静态定义好的。

【问题 2】

本题考查的是多媒体制作技术。

在 HTML 网页中可以插入多种多媒体素材，bmp 或 jpg 等是静态图像文件格式，而 flash 则是一种基于矢量的动画技术，用这种工具生成的动画文件可以插入网页中播放，从而实现动态显示效果。

【问题 3】

本题考查的是动态网页文件的格式。

ASP 书写的网页以.asp 作为扩展名，当服务器遇到以此为扩展名的文件就会对该文件中的 ASP 代码进行翻译，以生成纯 HTML 文档供 Web 浏览器显示。

【问题 4】

本题考查的是三层 B/S 网络计算的体系结构，

由 Web 浏览器和 Web 服务器构成的 Web 计算系统称为 B/S 系统，当应用程序的功能更为复杂时，可以在两者中间添加第三层，用于实现应用程序逻辑和配置。中间层可以是数据库，也可以是独立的应用服务器。

【问题 5】

本题考查的是 HTML 和 ASP 编程的语法知识。

我们常说，ASP 并不是一种语言，尽管看起来 ASP 的代码是以脚本的形式出现。Microsoft 把 ASP 定义为一个脚本语言执行的环境。在 HTML 语言里，标示一个标签是用尖括号，在 ASP 语言里其实没有什么不同，惟一的区别仅仅是使用<%%>来表示一个 ASP 的脚本语言的开始和结尾。

【问题 6】

本题考查的是动态网页中数据库连接方面的知识。

在 ASP 中连接 Access 数据库常用 Access OLE DB 连接方法，具体如下。

```
strconn = "DRIVER=Microsoft Access Driver (*.mdb);DBQ=" & Server.MapPath
("aspfree.mdp")
```

```
set conn = server.createobject("adodb.connection")
conn.open strconn
```

【问题 7】

本题考查的是动态网页中 ASP 代码向 HTML 代码转换方面的知识。

答案：

【问题 1】

(1) A

【问题 2】

(2) A

【问题 3】

(3) B

【问题 4】

(4) D

【问题 5】

(5) A　　(6) A　　(7) D　　(8) C　　(9) A

【问题 6】

数据库连接引擎：Microsoft.Jet.OLEDB.4.0

数据库文件名：Main.mdb

【问题 7】

```
<a href="http://www.baidu.com"target="_blank">百度</a>
```

例 7　阅读下列说明，根据网页显示的效果图，回答问题 1～问题 3。(2006 年 11 月下午试题五)

【说明】

某商务网站用 ASP 实现了一个在线手机性能评价投票网页，主页文件名为 inder.asp，用 IE 打开该网页后的效果如图 5-11 所示。程序中使用的 Access 数据表 Vote 结构如表 5-9 所示。



(a)



(b)

图 5-11　在线手机性能评价投票系统显示效果

表 5-9　Access 数据表结构

字 段 名	类　型	备　注
content	文本	选项文字标签
count	数字	投票数

index.asp 文档的内容如下：

```
<html>
<head>
<title>投票程序</title>
<%
Set cnn=Server.CreateObject("ADODB.Connection")
Set rec= Server.CreateObject("ADODB.Recordset")
cnn.ConnectionString="Driver={Microsoft  Access  Driver
(*.mdb)};Uid=;Pwd=;DBQ="  &
Server.MapPath("data.mdb")
cnn.  (1)  
dim rsql
rsql=  (2)  
rec.open rsql,cnn,3,3
rec.movefrist()
%>
</head>
<body>
<form name="piao" action="results.asp" method="post">
  <table width="237" border="1" align="center">
  <tr>
      <td valign=top width="216">
         <p align="center">  (3)  
      </td>
  </tr>
  <tr>
      <td valign=top width="216">
         <font size="2">
           (4)  
<%
  dim num
  num=0
  do while not rec.eof
  num=num+1
%>
<Input name='rd' type='radio' value='<%=num%>' id='<%=num%>'<%if num=1 then
response.write"checked"%>>
           <%=rec.field("content")%>
<%
  Rec.  (5)  
  Loop
```

```
%>
        </font>
       </td>
  </tr>
  <tr>
        <td valign=top width="216">
          <input name="submit00" type="submit" id="submit00" value="投票
">
        </td>
  </tr>
</table>
</body>
</html>
```

【问题 1】(每空 2 分，共 10 分)

从以下备选答案中为程序中(1)～(5)处空缺内容选择正确答案，填入答题纸对应的解答栏内。

(1) A. CreatObject()　　B. connect()　　C. go()　　D. open()

(2) A. "select*form data"　　B. "select*form vote"

C. select*form data　　D. select*form vote

(3) A. <pic border="0" src="mobile.bmp">

B. <picture border="0" src="mobile.bmp">

C. <img border="0" src="mobile.bmp">

D. <image border="0" src="mobile.bmp">

(4) A. <p align="left">您认为这款手机的性能如何？</p>

B. <p align="center">您认为这款手机的性能如何？</p>

C. <t align="left">您认为这款手机的性能如何？</t>

D. <t align="center">您认为这款手机的性能如何？</t>

(5) A. first()

B. next()

C. movenext()

D. nextrecord()

【问题 2】(2 分)

用户单击了【投票】按钮后，浏览器会执行什么操作？

【问题 3】(3 分)

如果希望运行 index.asp 后所得的结果如图 5-10 所示，三个单选按钮分别居中显示且让【一般】单选按钮作为默认选项，应该如何修改加粗部分的源代码。

分析：

【问题 1】

通过阅读程序，可以发现空(1)处需要填写的是一个打开数据库连接的函数，空(2)处需要填写存储数据库 SQL 查询的字符串变量 rsql 的内容，空(3)处需要填写图 5-11(a)中手机图

片对应的 HTML 代码，空(4)处需要填写如图 5-11(b)所示的文字“您认为这款手机的性能如何？”对应的 HTML 代码，空(5)处需要填写将数据库记录下移一条的 ASP 函数。因此解答为：(1)D　(2)B　(3)C　(4)A　(5)C。

【问题 2】

通过阅读程序发现：【投票】表单按钮<input name="submit00" type="submit" id="submit00" value="投票">位于<form name="piao" action="results.asp" method="post">中，因此单击该按钮将激活该 form 中定义的操作，因为其 action 属性的值为“results.asp”，所以将会运行 results.asp 程序。因此解答为浏览器运行 results.asp 文件，并在当前窗口中显示运行结果。

【问题 3】

如果希望运行 index.asp 后所得的结果如图 5-11(b)所示，可以发现图 5-11(b)与图 5-11(a)的不同之处在于三个单选按钮分行居中显示且让【一般】单选按钮作为默认选项。这时需要让每个按钮加上让其分行居中的代码，并且为【一般】单选按钮加上 default 属性。

答案：

【问题 1】

(1)　D

(2)　B

(3)　C

(4)　A

(5)　C

【问题 2】

浏览器运行 results.asp 文件，并在当前窗口中显示运行结果。

【问题 3】

将加粗部分的源代码修改为：

```
<p align="center">
      <Input name='rd' type='radio' value='<%=num%>' id='<%=num%>' <%if
num=2 then response.write "checked"%>>
      <%=rec.fields("content")%>
</p>
```

例 8　阅读下列说明，根据网页显示的效果图，补充 ASP 程序中各空格处空缺的代码，解释程序中用下画线标出的语句的含义，将解答填入答题纸对应的解答栏内。(2006 年 5 月下午试题五)

【说明】

某在线娱乐公司用 ASP 实现了一个用于在线点播电影的网页，主页文件名为 index.asp，网页运行的效果如图 5-12 所示。程序中使用的 Access 数据表结构如表 5-10 和表 5-11 所示。



图 5-12 在线电影系统显示效果

表 5-10 data 数据表结构

字 段 名	类 型	备 注
id	自动编号	编号
name	文本	电影名字
type	文本	播放格式
item	文本	电影类型
hits	数字	单击次数
mark	文本	推荐度
date	日期/时间	加入时间

表 5-11 item 数据表结构

字 段 名	类 型	备 注
id	自动编号	编号
name	文本	类型条目名称

conn.asp 文档的内容如下：

```
 <%
 dimdb,conn,connstr
 db="film.mdb"
 set Conn=server.CreateObject("ADODB.connection")
connstr="provider=microsoft.jet.oledB.4.0;data
source="&server.MapPath("data/"&db&"")
     conn.Open connstr       <!--第(1)处--> (2 分)
 %>
```

index.asp 文档的内容如下。

```
 (2)          <!--第(2)处--> (1 分)
<html>
<head>
<title>在线电影</title>
<style type="text/css">
<!--
td          {font-size:12px;line-height:17px}
body        {font-size:12px;line-height:17px}
p           {margin-top:1px;margin-bottom:1px}
a:link      {text-decoration:none;color:black}
a:visited   {text-decoration:none;color:black}
a:active    {text-decoration:none;color:blue}  <!--第(3)处-->(2 分)
-->
</style>
</head>
<body leftmargin="0" topmargin ="0">
<!--#include file="head.asp"-->
<div align="center">               <!--第(4)处--> (2 分)
<table>
  <td height="30" width="367">
    <%sql="select * from item"
      set rs_item=server.createobject("adodb.recordset")
      rs_iterm.open sql,connstr,1,1
      response.write"<p><b><img src=images/dot1.gif><a href=index.asp>全
部电影</a> "
      do while not rs_item.eof
        response.write "<img src=images/dotl.gif border=0><a
href=index.asp?item="
&rs_item("name")&">"&rs_itern("name")&"</a> "
        ____(5)____      <!--第(5)处--> (1 分)
      loop             <!--第(6)处--> (2 分)
      response.write "</b> "
      rs item.close%>
  </td>
</table>
</div>

<div align="center">
<% dim item_type
  item_type= ____(7)____        <!--第(7)处--> (1 分)
  if item_type="" or itcrn_type ="全部电影" then
    sql="sclect * from data"
  else
    sql="____(8)____"           <!--第(8)处--> (1 分)
  end if
  set rs=server. createobject("adodb.recordset")
  rs.open sql,connslr,1,1
```

```
 %>
 <table
   <tr>
     <td width="125" background="images/bg.gif" height="30"> 
     <img border="0" src="images/biao_lefi.gif" width=" 15" height=" 15">
影片名字</td>
     <td width="115' background="images/bg.gif" height="30"
align=''center''>在线播放</td>
     <td width="64" background--"images/bg.gif" height="30" align="center">
电影类型</td>
     <td width="58" background="images/bg.gif" height="30" align="center">
播放格式</td>
     <td width="43" background-"images/bg, gif" heighr="30" align="center">
单击</td>
     <td width="70" background="images/bg.gif" height="30" align="center">
加入日期</td>
     <td width="73" background="images/bg, gif" height="30" align="center">
推荐度</td>
   </tr>
 <%do while not rs.eot%>
   <tr>
     <td width="125" height"30" > <img border="0"
src="images/dian.gif"> 
     <%=rs( "name" )%></rd>
       <td width=" 115" height="30" align="center"><a href="">点播</td>
       <td width="64" heigh-t="30" align ="center"><a
href="index.asp?item=<%=rs("item")%>">
     <%=rs("item")%></td>
       <td width="58'' height="30" align="center"><%=rs("type")%></td>
       ____(9)____          <!--第(9)处--> (1 分)
       <td width="70" height="30" align="center"><%=rs("date")%</td>
       <td width="73" height="30" align="center"><font
color="red"><%=rs("mark")%></a></td>
  </tr>
 <% rs.movenext          <!--第(10)处-->    (2 分)
   loop%>
 </table>
 </div>
 <!--#include file="foot.asp"-->
 </body>
 </html>
```

分析：

本题考查的是有关 HTML 网页制作和 ASP 编程方面的知识。

空(1)处，conn.asp 文件的作用是打开数据库，前面定义数据库连接对象 conn 和连接字符串 connstr，此处是打开数据库连接。

空(2)处的作用是将 conn.asp 文件包含在 index.asp 文件中，因此就应填入

```
<!--#include file="conn.asp"-->
```

空(3)处的作用是定义样式表，当前处于活动状态的标签<a>中的文字显示为蓝色。
空(4)处，align="center"说明了<div>标记下的内容居中。
空(5)处的作用是将数据集对象 rs_item 移动到下一条记录，因此应填写

```
rs_item.movenext
```

空(6)处，do while……loop 构成了一个循环，loop 的作用是转下一轮循环。
空(7)处的作用是引用 request("item")，但需要去除空格，因此应填写

```
trim(request("item"))
```

空(8)处应填写一个 SQL 语句，以查找符号条件的记录，因此应填写

```
select *from data where item="&item_type&"
```

空(9)处的作用是在表格中显示这部电影的“单击次数”，

```
<td width="#" height="30" align="cener"><%=rs("hits")%></td>
```

需要注意，#是指定宽度，但高度 height 必须和前几个字段一样，也是 30。
空(10)处，rs.movenext 的作用是将数据集对象 rs 移动到下一条记录。

答案：

(1) 数据库连接对象 conn 以 connstr 中定义的连接字符串打开数据库连接
(2) <!--#include file="conn.asp"-->
(3) 当前处于活动状态的标签<a>中的文字显示为蓝色
(4) <div>标记下的内容居中
(5) rs_item.movenext
(6) 转下一次 while 循环
(7) Trim(request("item"))
(8) select * from data where item="&item_type&"
(9) <td width="43"height="30"align="center"><%=rs("hits")%></td>
(10) 数据集对象 rs 移动到下一条记录

5.2.3　同步练习

请根据网页显示的效果图和网页中的元素说明，将 HTML 文本中各空格处的解答填入答案的对应栏中。

【说明】

在 IE 浏览器中输入 yoyo 电子邮局主页地址并按 Enter 键后，网页的显示效果如图 5-13 所示。



图 5-13 yoyo 电子邮局主页在 IE 中刚打开时的效果

网页中各元素说明如下。

序 号	类 型	说 明
(1)	图片	文件名：“atmail.jpg”；宽度：80pixels；高度：80pixels
(2)	【登录名：】文本框	名称：“login_name”；尺寸：20 字符
(3)	【密码：】文本框	名称：“login_password”；尺寸：20 字符
(4)	【类型：】下拉列表框	下拉列表项：“商务用户”、“VIP 用户”、“免费用户”
(5)	发送电子邮件超链接	邮件发送地址：“vipmail@yoyo.net”
(6)	BBS 超链接	超链接地址：“http://bbs.yoyo.com”

HTML 文本如下：

```
<html>
<head>
<title>yoyo 邮局主页</title>
</head>
<body>
<p align="center">
<b><font color="#800080" face="楷体_GB2312" size="5">yoyo 邮局</font></b>
</p>
<p align="center">
___________(1)___________
</p>
<p align="left"> </p>
<p align="left">用户登录</p>
<table>
    <tr><td width="100" height="16">
        <div align="right">
            登录名：
        </div></td>
```

```
        ____________(2)____________
</table>
<table>
    <tr><td width="100" height="16">
        <div align="right">
            密　码:
        </div></td>
        ____________(3)____________
</table>
<table>
    <tr><td width="100">
        <div align="right">
            类　型:
        </div></td>
        <select onchange="changeBackURL()" name="select">
            <option>商务用户</option>
            ____________(4)____________
            <option>免费用户</option>
        </select>
</table>
    <p></p><p></p>
    VIP 服务咨询邮箱: ____________(5)____________
    <a href="http://bbs.yoyo.com">参加 yoyo 邮局社区讨论</a>
</body>
</html>
```

5.2.4　同步练习参考答案

(1)　<img src="atmail.jpg"width="80" height="80">

(2)　<input name="login_name"size="20">

(3)　<input type="password" name="login_password" size="20">

(4)　<option selected>VIP 用户</option>

(5)　vipmail@yoyo.net

5.3　Web 网站的创建与维护

5.3.1　考点辅导

5.3.1.1　Web 网站的创建

1. 组织信息

创建 Web 网站时，需要考虑网站的扩展性、网页技术和网页制作工具的选择，同时还必须考虑网站信息分解、网页链接、主题列表和逻辑顺序等，确保做好网站规划。

2. 构建网站框架

构建网站框架时，可以考虑采用布告板、单页线性、多页线性、分层和网状等逻辑组织形式，以提高网站的编码效率。

3. 建立Web服务器

(1) Web服务器简介

Web服务器是用来存储网页并响应执行用户的访问请求的设备。Web服务器对通过因特网使用HTTP协议的文件、文件夹以及其他资源的访问进行管理，当前最流行的两种Web服务器是运行于Linux操作系统平台上的Apache Web服务器和运行于Windows操作系统平台上的Microsoft的IIS Web服务器。

获得Web服务器空间的方式主要包括企业或单位自建和托管Web主机两种方式。企业或单位安置服务器需要相应的硬件、软件，还需要相关的人员来架设并维护Web服务器。

(2) IIS Web服务器

利用IIS的主要功能可以设置个人Web服务器，在工作组中共享信息，访问数据库，开发企业Intranet和开发Web应用程序。

用户可以通过Windows的计算机管理控制台或通过编写脚本来管理IIS。还可以使用控制台，通过Web与他人共享使用Internet信息服务管理的站点和服务器的内容。从控制台访问Internet信息服务器，可以配置最常用的IIS设置和属性。开发站点和应用程序之后，可以在运行功能更加强大的Windows Server环境中使用这些设置和属性。

4. 域名注册

域名解析服务器主要负责将Web或其他服务器域名解析为相应的IP地址。选择适当的域名后，就可以到中国互联网络信息中心进行注册域名，并签订相应的域名注册协议。

5. Web网站发布

网站发布之前需要准备Web服务器的相关信息，主要包括Web服务器协议、URL地址、服务器文件系统规则和服务器帐号等。实施Web发布时，可以采用FTP工具将网站文件从本地传输到远程服务器上。

5.3.1.2 Web网站的维护

1. 网站维护

网站维护主要涉及网站系统平台维护和网站内容更新维护两个主要方面。

2. 网站测试

网站测试的主要内容包括浏览器的可变性、不同的分辨率和链接的有效性等。

5.3.2 典型例题分析

例1 请根据网页显示的效果图和网页中的元素说明，将HTML文本中各空格处的解答填入对应的答案栏内。

【说明】

在浏览器的地址栏中输入常春藤大学招生办公室主页的网址并按 Enter 键后，网页显示的效果如图 5-14 所示。

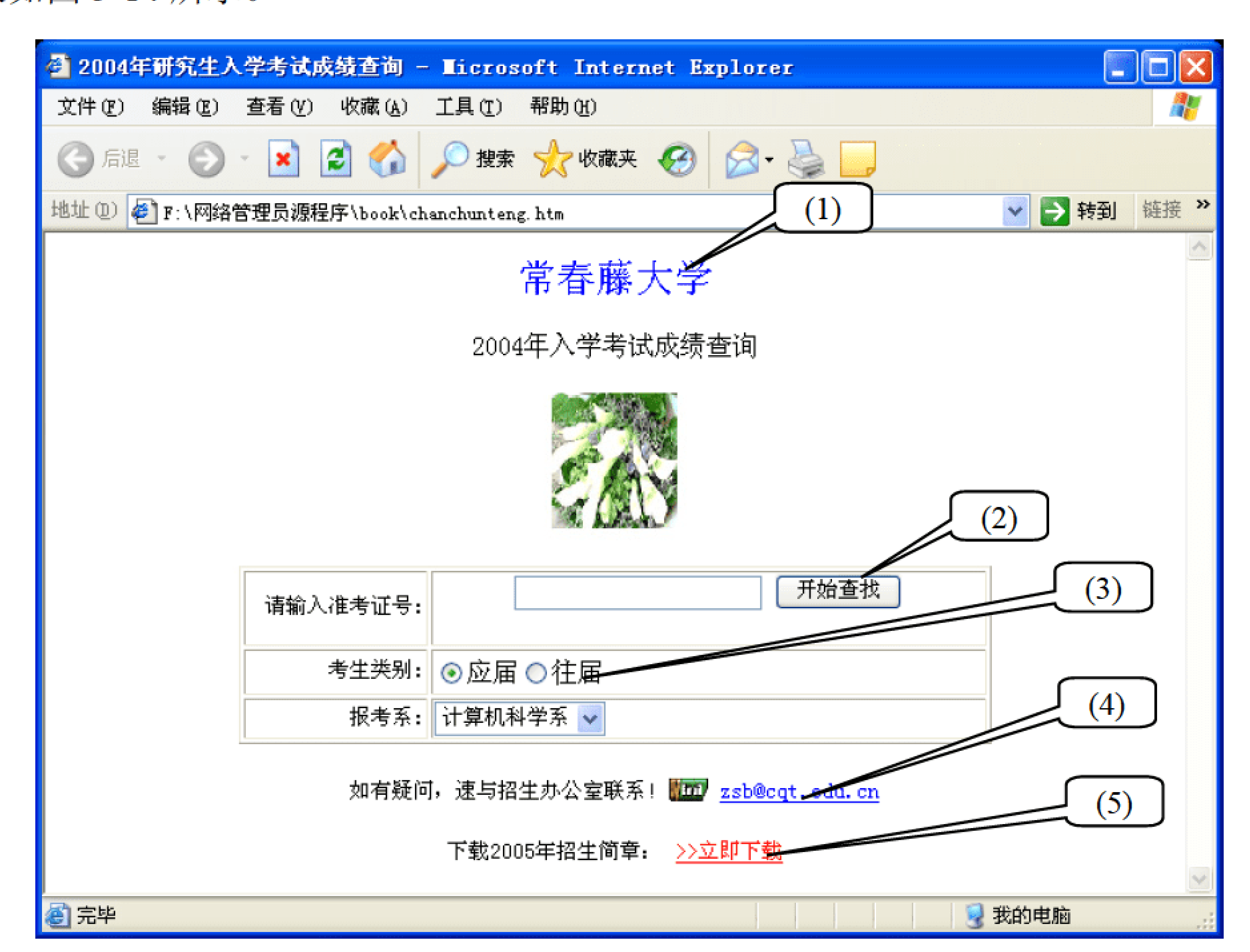


图 5-14　常春藤大学招生办公室主页

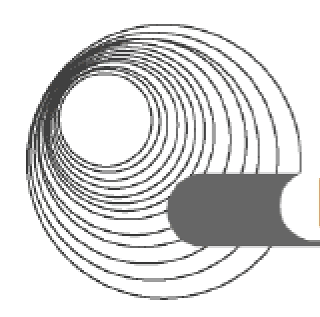
网页中的元素说明如下。

序　号	类　型	说　明
(1)	文本	内容：常春藤大学；颜色：blue；字体：宋体；字号：5
(2)	表单	方法：post；程序：http://www.server.com/cgibin/program
(3)	【考生类别：】选项组	名称：“type”；选项：“应届”、“往届”
(4)	动画	文件名：animation.gif；高：16；宽：24
(5)	【立即下载】链接	文件地址：http://download.cqt.edu.cn/zsjz2005.doc

HTML 文本如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>2004 年研究生入学考试成绩查询</title>
      (1)

<body  bgcolor="white">
       (2)
</p>
<p align="center">2004 年入学考试成绩查询</p>
```




```
<p align="center"><img src="nyc.jpg" width="77" height="83">
</p>
<div  align="center" style="width:679; height:101 ">
<table width="63%" height="17" border="1" >
    <tr>
      <td width="23%" height="1">
       <p align="right"><font face="宋体" size="2">请输入准考证号:</font></p>
       </td>
      <td width="46%" height="1">
    ______(3)______
       <p align="left">
       <input type="text" name="T1" size="20">
       <input type="submit" value="开始查找" name="B1"></p>
       </form>
       </td>
    </tr>
    <tr>
      <td width="23%" height="17">
       <p align="right"><font size="2">考生类别:</font></p>
       </td>
      <td width="38%" height="19" align="left">
______(4)______
       </td>
    </tr>
    <tr>
      <td width="23%" height="1">
       <p align="right"><font size="2">报考系:</font></p>
       </td>
      <td width="46%" height="1">
       <p align="left"><select  size="1" name="D1">
       <option selected>计算机科学系</option>
       <option>机械工程系</option>
       <option>中文系</option>
      </select>
       </p>
       </td>
    </tr>
  </table>
</div>
<p align="center"><font size="2">如有疑问，速与招生办公室联系！
______(5)______
<a href="mailto:vipmail@cqt.edu.cn">zsb@cqt.edu.cn</a></font>
</p>
<p align="center"><font size="2">下载 2005 年招生简章：</font>
______(6)______
<font size="2" color="red"> &gt;&gt;立即下载</font></a></p>
</body>
</html>
```

分析：本题主要考查考生对 HTML 网页元素标签的掌握情况。

HTML 元素主要包括基本标签(如字体)、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题中主要涉及字体、表单、单选按钮、图像和文档下载的超级链接等基本元素。

答案：

(1) </head>

(2) 常春藤大学

(3) <form name="frmSearch"method="post"action="http://www.server.com/cgibin/ program">

(4) <input name="type" type="radio" value="应届" checked>应届
<input name="type" type="radio"　value="往届">往届

(5) <img src="animation.gif" width="24"　height="16" align="absmiddle">

(6) <a href="http://download.cqt.edu.cn/zsjz2005.doc">

5.3.3　同步练习

请根据网页显示的效果图(见图 5-15)和网页中的元素说明，将 HTML 文本中各空格处的解答填入对应的答案栏中。

网页中元素说明如下。

序　号	类　型	说　明
(1)	网页标题	文本：Form 表单示例
(2)	表单对象	Name：frmLogin；method：post；action：login.aspx
(3)	输入文本框	Name：txtUser；Id：txtUser
(4)	文本标签	Label：class：style1；文本：密 码
(5)	复选框	Checkbox：checked；name：eem

这是一个简单的 HTML 文档，显示的是一个网页列表信息，显示界面如图 5-15 所示。

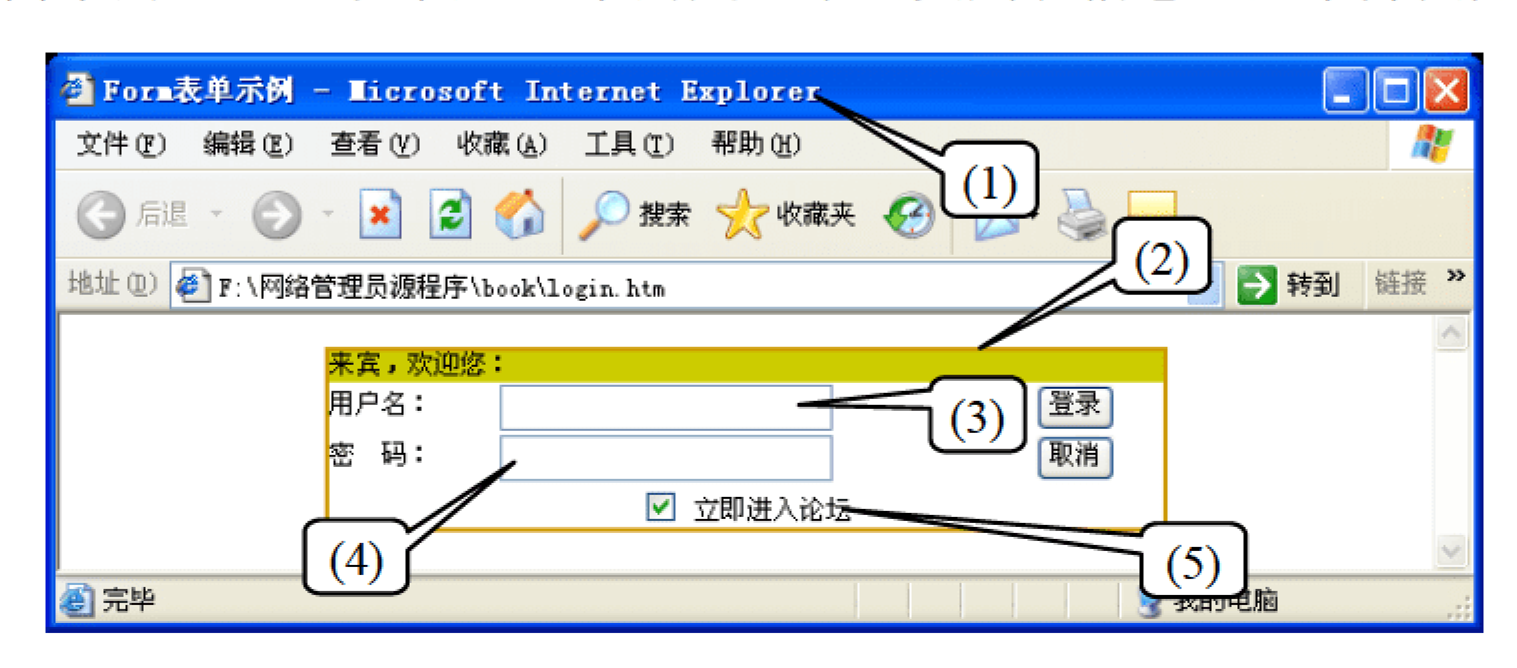
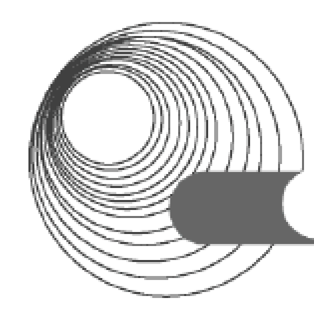


图 5-15　论坛网页

下面是这个论坛页面的 HTML 代码：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```




```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
____(1)________
<style type="text/css">
<!--
.style1 {
    font-family: "宋体";
    font-size: 12px;
}
-->
</style>
</head>
<body>
__________(2)______________
  <table width="200" border="1" align="center" cellpadding="0"
cellspacing="0" bordercolor="#CC9900">
    <tr>
    <td>
    <table width="381" border="0" align="center" cellpadding="0"
cellspacing="0" bordercolor="#D4D0C8">
   <tr>
     <td colspan="3" bgcolor="#CCCC00" scope="col"><span class="style1">
来宾，欢迎您：</span></td>
    </tr>
   <tr>
     <td scope="col"><label class="style1">用户名：</span></label></td>
     <td scope="col">____(3)______</td>
     <td scope="col"><div align="left">
       <input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=登录>
     </div></td>
   </tr>
   <tr>
     <td>____(4)______</td>
     <td><input name="txtPasswd" type="text" id="txtPasswd"></td>
     <td><input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=取消></td>
   </tr>
   <tr>
     <td colspan="3"><div align="center" class="style1">
        _______(5)_______
     立即进入论坛</div></td>
   </tr>
  </table>
```

```
      </td>
    </tr>
    </table>
  </form>
  </body>
  </html>
```

5.3.4　同步练习参考答案

(1)　<title>Form 表单示例</title>

(2)　<form name="frmLogin" method="post" action="login.aspx">

(3)　<input name="txtUser" type="text" id="txtUser">

(4)　<label class="style1">密　码：</label>

(5)　<input type=checkbox checked name=eem>

5.4　本 章 小 结

本章知识点在 2009 年的新大纲中改动不大，主要删除了 XML 动态网页编程技术知识点，新增了 ADO 的概念和实用的知识点。

本部分内容主要要求考生掌握 Web 网站建设的相关内容，包括 HTML 的基础知识，HTML 应用，网页制作工具使用，动态网页技术以及 Web 网站的建立、管理和维护等 Web 基础知识和应用实现等内容。对 Web 网站建设的学习关键要充分掌握 HTML 的基础知识，以常用的 HTML 元素为主线，抓住重点，熟悉 Web 网站建设中的动态网页技术使用和网站管理与维护等相关内容。

本章内容为下午科目的重点内容，为每年的必考内容。本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点。

5.5　达标训练题及参考答案

5.5.1　达标训练题

要定义显示一个如图 5-16 所示的网页表格，相关信息参考下面的网页说明。将 HTML 文本中各空格处的解答填入对应栏中。

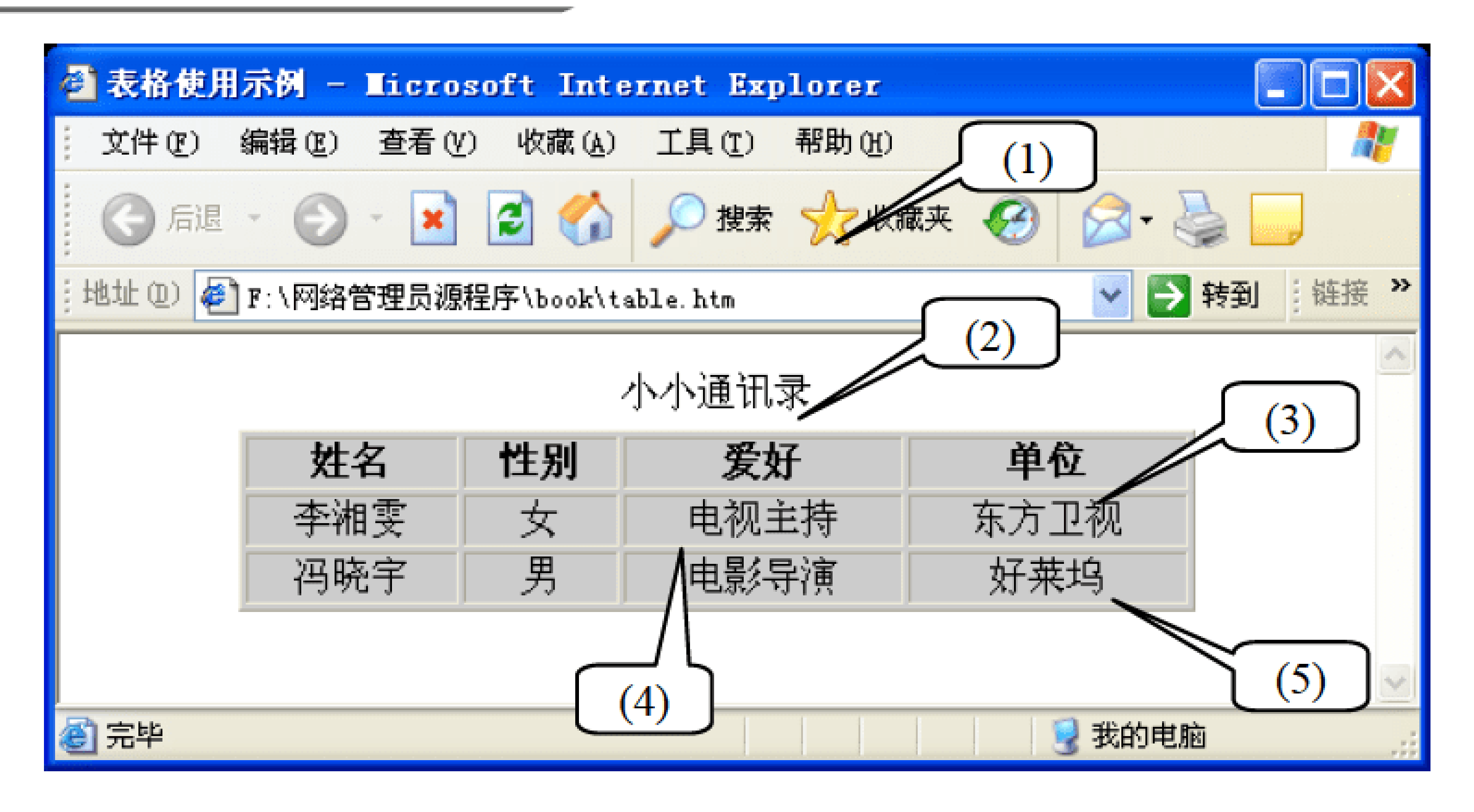


图 5-16 表格在浏览器中打开的效果

网页中各元素的说明如下。

序 号	类 型	说 明
(1)	网页标题	文本：表格使用示例
(2)	表格标题	文本：小小通讯录
(3)	单元格标题	内容：单位 对齐方式：居中
(4)	单元格内容	内容：电视主持 对齐方式：居中
(5)	表格结束	表格结束 HTML 标签

HTML 文本如下：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
 ____________(1)____________
</head>
<body>
<table width="200" border="1" bgcolor="#CCCCCC" align="center">
____________(2)____________
<thead>
  <tr>
    <th align="center">姓名</th>
    <th align="center">性别</th>
    <th align="center">爱好</th>
    ____________(3)____________
  </tr>
 </thead>
 <tbody>
  <tr>
    <td align="center">李湘雯</td>
    <td align="center">女</td>
    ____________(4)____________
```

```
    <td align="center">东方卫视</td>
  </tr>
  <tr>
    <td align="center">冯晓宇</td>
    <td align="center">男</td>
    <td align="center">电影导演</td>
    <td align="center">好莱坞</td>
  </tr>
 </tbody>
____________(5)____________
</body>
</html>
```

5.5.2　参考答案

(1)　<title>表格使用示例</title>

(2)　<caption>小小通讯录</caption>

(3)　<th align="center">单位</th>

(4)　<td align="center">电视主持</td>

(5)　</table>

参 考 文 献

1. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络管理员教程(第 3 版)[M]. 北京：清华大学出版社，2009
2. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络管理员考试同步辅导[M]. 北京：清华大学出版社，2005
3. 全国计算机技术与软件专业技术资格(水平)考试办公室编．2009 年网络管理员考试大纲与培训指南(2009 版)[M]. 北京：清华大学出版社，2009
4. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络管理员历年试题分析与解答[M]. 北京：清华大学出版社，2008
5. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络工程师历年试题分析与解答[M]. 北京：清华大学出版社，2008
6. 雷震甲．网络工程师教程(第 3 版)[M]. 北京：清华大学出版社，2009
7. 谢希仁．计算机网络(第 5 版)[M]．北京：电子工业出版社，2009
8. 李保华，李敏. 局域网组建与维护(2009 版)[M] ．北京：清华大学出版社，2009
9. 王俊伟，吴俊海. Linux 标准教程[M]．北京：清华大学出版社，2006
10. 冉林仓．Red Hat Linux 9 编程开发与网络管理[M]．北京：电子工业出版社，2006
11. 王全国等．网管实战宝典：Windows Server 2003 配置与管理[M]．北京：清华大学出版社，2008
12. 斯托林斯等．网络安全基础：应用与标准(第 3 版)[M]．北京：清华大学出版社，2007
13. 唐正军等. 入侵检测技术[M]．北京：清华大学出版社，2008
14. 鲍威尔. 数据库设计入门经典[M]．北京：清华大学出版社，2007
15. 白中英等．计算机组成原理[M]．北京：科学出版社，2008
16. 汤子瀛．计算机操作系统(修订版)．西安：西安电子科技大学出版社，2001
17. 康雁等．计算机专业英语：使用文案(档)写作[M]．北京：清华大学出版社，2009
18. 胡静等．ASP.NET 动态网站开发教程(第 2 版)[M]．北京：清华大学出版社，2009
19. 《计算机信息网络国际联网安全保护管理办法》(1997 年 12 月 30 日中华人民共和国公安部令第 33 号发布)
20. 《计算机信息系统安全专用产品检测和销售许可证管理办法》(1997 年 12 月 12 日公安部令第 32 号发布)
21. 《计算机信息系统国际联网保密管理规定》(2000 年 1 月 25 日国家保密局国保发[1999]10 号发布)
22. 《中华人民共和国计算机信息系统安全保护条例》(1994 年 2 月 18 日中华人民共和国国务院令第 147 号发布)